

# All Artifacts for the paper “Achilles’ Heel of Plug-and-Play Software Architectures: A Grounded Theory Based Approach”

## Table of Contents

- [AllRetrievedData](#): All the CVEs that were retrieved from the National Vulnerability Database (Section 3.2.2). These vulnerability reports are released as CSV files containing:
  - cve\_id (vulnerability identifier)
  - description (description of the security issue)
- [FilteredCVEs](#): The output of our three complementary filtering approach (Section 3.2.3). The output for each project is an Excel Sheet that contains:
  - cve\_id (vulnerability identifier)
  - keyword-based (This column has an “X” if the CVE matched the heuristic of the keyword-based approach. Otherwise, it has a N/A)
  - component-based (This column has an “X” if the CVE matched the heuristic of the component-based approach. Otherwise, it has a N/A)
  - file-based (This column has an “X” if the CVE matched the heuristic of the file-based approach. Otherwise, it has a N/A)
- [CVESummaries](#): The tables with the CVE summaries (context, problem, solution) as well as the augmenting links (commit url, and issue tracking system URL) that we manually collected.
- [CodedCVEs](#): The analyzed CVEs with highlights of the keypoints as well as their corresponding codes. There is also an Excel Sheet with the frequencies of each code per software project.
- [Core Categories Mapped to CVEs](#): This folder has the list of CVEs per core category (i.e, type of plug-and-play vulnerability).
- [Memos](#): It contains the notes taken throughout the data analysis ("memoing").
- [Theoretical Codes](#): The results of our theoretical coding process. Glaser (1978) proposes 18 coding families, in which case we chose a minified version of six C that only included context, consequences, contingencies (mitigations).

## All Retrieved Data

### Chromium CVEs

cve_id	description
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-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-2008-4340	Google Chrome 0.2.149.29 and 0.2.149.30 allows remote attackers to cause a denial of service (memory consumption) via an HTML document containing a carriage return ("\\r\\n\\r\\n") argument to the window.open function.
CVE-2008-4724	Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome 0.2.149.30 allow remote attackers to inject arbitrary web script or HTML via an ftp:// URL for an HTML document within a (1) JPG, (2) PDF, or (3) TXT file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2008-5749	** DISPUTED ** Argument injection vulnerability in Google Chrome 1.0.154.36 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI. NOTE: a third party disputes this issue, stating that Chrome "will ask for user permission" and "cannot launch the applet even [if] you have given out the permission."
CVE-2008-5915	An unspecified function in the JavaScript implementation in Google Chrome creates and exposes a "temporary footprint" when there is a current login to a web site, which makes it easier for remote attackers to trick a user into acting upon a spoofed pop-up message, aka an "in-session phishing attack." NOTE: as of 20090116, the only disclosure is a vague pre-advisory with no actionable information. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.
CVE-2008-6994	Stack-based buffer overflow in the SaveAs feature (SaveFileAsWithFilter function) in win_util.cc in Google Chrome 0.2.149.27 allows user-assisted remote attackers to execute arbitrary code via a web page with a long TITLE element, which triggers the overflow when the user saves the page and a long filename is generated. NOTE: it might be possible to exploit this issue via an HTTP response that includes a long filename in a Content-Disposition header.
CVE-2008-6995	Integer underflow in net/base/escape.cc in chrome.dll in Google Chrome 0.2.149.27 allows remote attackers to cause a denial of service (browser crash) via a URI with an invalid handler followed by a "%" (percent) character, which triggers a buffer over-read, as demonstrated using an "about:%" URI.
CVE-2008-6996	Google Chrome BETA (0.2.149.27) does not prompt the user before saving an executable file, which makes it easier for remote attackers or malware to cause a denial of service (disk consumption) or exploit other vulnerabilities via a URL that references an executable file, possibly related to the "ask where to save each file before downloading" setting.
CVE-2008-6997	Google Chrome 0.2.149.27 allows user-assisted remote attackers to cause a denial of service (browser crash) via an IMG tag with a long src attribute, which triggers the crash when the victim performs an "Inspect Element" action.
CVE-2008-6998	Stack-based buffer overflow in chrome/common/gfx/url_elider.cc in Google Chrome 0.2.149.27 and other versions before 0.2.149.29 might allow user-assisted remote attackers to execute arbitrary code via a link target (href attribute) with a large number of path elements, which triggers the overflow when the status bar is updated after the user hovers over the link.
CVE-2008-7061	The tooltip manager (chrome/views/tooltip_manager.cc) in Google Chrome 0.2.149.29 Build 1798 and possibly other versions before 0.2.149.30 allows remote attackers to cause a denial of service (CPU consumption or crash) via a tag with a long title attribute, which is not properly handled when displaying a tooltip, a different vulnerability than CVE-2008-6994. NOTE: there is inconsistent information about the environments under which this issue exists.
CVE-2008-7246	Google Chrome 0.2.149.29 and earlier allows remote attackers to cause a denial of service (unusable browser) by calling the window.print function in a loop, aka a "printing DoS attack," possibly a related issue to CVE-2009-0821.
CVE-2008-7294	Google Chrome before 4.0.211.0 cannot properly restrict modifications to cookies established in HTTPS sessions, which allows man-in-the-middle attackers to overwrite or delete arbitrary cookies via a Set-Cookie header in an HTTP response, related to lack of the HTTP Strict Transport Security (HSTS) includeSubDomains feature, aka a "cookie forcing" issue.

CVE-2009-0276	Cross-domain vulnerability in the V8 JavaScript engine in Google Chrome before 1.0.154.46 allows remote attackers to bypass the Same Origin Policy via a crafted script that accesses another frame and reads its full URL and possibly other sensitive information, or modifies the URL of this frame.
CVE-2009-0374	** DISPUTED ** Google Chrome 1.0.154.43 allows remote attackers to trick a user into visiting an arbitrary URL via an onclick action that moves a crafted element to the current mouse position, related to a "Clickjacking" vulnerability. NOTE: a third party disputes the relevance of this issue, stating that "every sufficiently featured browser is and likely will remain susceptible to the behavior known as clickjacking," and adding that the exploit code "is not a valid demonstration of the issue."
CVE-2009-0411	Google Chrome before 1.0.154.46 does not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls and other web script.
CVE-2009-1412	Argument injection vulnerability in the chromehtml: protocol handler in Google Chrome before 1.0.154.59, when invoked by Internet Explorer, allows remote attackers to determine the existence of files, and open tabs for URLs that do not satisfy the IsWebSafeScheme restriction, via a web page that sets document.location to a chromehtml: value, as demonstrated by use of a (1) javascript: or (2) data: URL. NOTE: this can be leveraged for Universal XSS by exploiting certain behavior involving persistence across page transitions.
CVE-2009-1413	Google Chrome 1.0.x does not cancel timeouts upon a page transition, which makes it easier for attackers to conduct Universal XSS attacks by calling setTimeout to trigger future execution of JavaScript code, and then modifying document.location to arrange for JavaScript execution in the context of an arbitrary web site. NOTE: this can be leveraged for a remote attack by exploiting a chromehtml: argument-injection vulnerability.
CVE-2009-1414	Google Chrome 2.0.x lets modifications to the global object persist across a page transition, which makes it easier for attackers to conduct Universal XSS attacks via unspecified vectors.
CVE-2009-1441	Heap-based buffer overflow in the ParamTraits<SkBitmap>::Read function in Google Chrome before 1.0.154.64 allows attackers to leverage renderer access to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to a large bitmap that arrives over the IPC channel.
CVE-2009-1442	Multiple integer overflows in Skia, as used in Google Chrome 1.x before 1.0.154.64 and 2.x, and possibly Android, might allow remote attackers to execute arbitrary code in the renderer process via a crafted (1) image or (2) canvas.
CVE-2009-1514	Google Chrome 1.0.154.53 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a throw statement with a long exception value.
CVE-2009-1598	Google Chrome executes DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file, which might allow remote attackers to bypass intended Adobe Acrobat JavaScript restrictions on accessing the document object, as demonstrated by a web site that permits PDF uploads by untrusted users, and therefore has a shared document.domain between the web site and this javascript: URI. NOTE: the researcher reports that Adobe's position is "a PDF file is active content."
CVE-2009-1690	Use-after-free vulnerability in WebKit, as used in Apple Safari before 4.0, iPhone OS 1.0 through 2.2.1, iPhone OS for iPod touch 1.1 through 2.2.1, Google Chrome 1.0.154.53, and possibly other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) by setting an unspecified property of an HTML tag that causes child elements to be freed and later accessed when an HTML error occurs, related to "recursion in certain DOM event handlers."
CVE-2009-2060	src/net/http_transaction_winhttp.cc in Google Chrome before 1.0.154.53 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx 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-2009-2071	Google Chrome before 1.0.154.53 displays a cached certificate for a (1) 4xx or (2) 5xx CONNECT response page returned by a proxy server, which allows man-in-the-middle attackers to spoof an arbitrary https site by letting a browser obtain a valid certificate from this site during one request, and then sending the browser a crafted 502 response page upon a subsequent request.
CVE-2009-2121	Buffer overflow in the browser kernel in Google Chrome before 2.0.172.33 allows remote HTTP servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted response.
CVE-2009-2352	Google Chrome 1.0.154.48 and earlier does not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header, a related issue to CVE-2009-1312. NOTE: it was later reported that 2.0.172.28, 2.0.172.37, and 3.0.193.2 Beta are also affected.
CVE-2009-2555	Heap-based buffer overflow in src/jsregexp.cc in Google V8 before 1.1.10.14, as used in Google Chrome before 2.0.172.37, allows remote attackers to execute arbitrary code in the Chrome sandbox via a crafted JavaScript regular expression.
CVE-2009-2556	Google Chrome before 2.0.172.37 allows attackers to leverage renderer access to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors that trigger excessive memory allocation.
CVE-2009-2578	Google Chrome 2.x through 2.0.172 allows remote attackers to cause a denial of service (application crash) via a long Unicode string argument to the write method, a related issue to CVE-2009-2479.

CVE-2009-2816	The implementation of Cross-Origin Resource Sharing (CORS) in WebKit, as used in Apple Safari before 4.0.4 and Google Chrome before 3.0.195.33, includes certain custom HTTP headers in the OPTIONS request during cross-origin operations with preflight, which makes it easier for remote attackers to conduct cross-site request forgery (CSRF) attacks via a crafted web page.
CVE-2009-2935	Google V8, as used in Google Chrome before 2.0.172.43, allows remote attackers to bypass intended restrictions on reading memory, and possibly obtain sensitive information or execute arbitrary code in the Chrome sandbox, via crafted JavaScript.
CVE-2009-2955	Google Chrome 1.0.154.48 and earlier allows remote attackers to cause a denial of service (CPU consumption and application hang) via JavaScript code with a long string value for the hash property (aka location.hash), a related issue to CVE-2008-5715.
CVE-2009-2973	Google Chrome before 2.0.172.43 does not prevent SSL connections to a site with an X.509 certificate signed with the (1) MD2 or (2) MD4 algorithm, which makes it easier for man-in-the-middle attackers to spoof arbitrary HTTPS servers via a crafted certificate, a related issue to CVE-2009-2409.
CVE-2009-2974	Google Chrome 1.0.154.65, 1.0.154.48, and earlier allows remote attackers to (1) cause a denial of service (application hang) via vectors involving a chromehtml: URI value for the document.location property or (2) cause a denial of service (application hang and CPU consumption) via vectors involving a series of function calls that set a chromehtml: URI value for the document.location property.
CVE-2009-3011	Google Chrome 1.0.154.48 and earlier, 2.0.172.28, 2.0.172.37, and 3.0.193.2 Beta does not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: the JavaScript executes outside of the context of the HTTP site.
CVE-2009-3263	Cross-site scripting (XSS) vulnerability in Google Chrome 2.x and 3.x before 3.0.195.21 allows remote attackers to inject arbitrary web script or HTML via a (1) RSS or (2) Atom feed, related to the rendering of the application/rss+xml content type as XML "active content."
CVE-2009-3264	The getSVGDocument method in Google Chrome before 3.0.195.21 omits an unspecified "access check," which allows remote web servers to bypass the Same Origin Policy and conduct cross-site scripting attacks via unknown vectors, related to a user's visit to a different web server that hosts an SVG document.
CVE-2009-3268	Google Chrome 1.0.154.48 and earlier allows remote attackers to cause a denial of service (CPU consumption) via an automatically submitted form containing a KEYGEN element, a related issue to CVE-2009-1828.
CVE-2009-3456	Google Chrome, possibly 3.0.195.21 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. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2009-3931	Incomplete blacklist vulnerability in browser/download/download_exe.cc in Google Chrome before 3.0.195.32 allows remote attackers to force the download of certain dangerous files via a "Content-Disposition: attachment" designation, as demonstrated by (1) .mht and (2) .mhtml files, which are automatically executed by Internet Explorer 6; (3) .svg files, which are automatically executed by Safari; (4) .xml files; (5) .htt files; (6) .xsl files; (7) .xslt files; and (8) image files that are forbidden by the victim's site policy.
CVE-2009-3932	The Gears plugin in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service (memory corruption and plugin crash) or possibly execute arbitrary code via unspecified use of the Gears SQL API, related to putting "SQL metadata into a bad state."
CVE-2009-3933	WebKit before r50173, as used in Google Chrome before 3.0.195.32, allows remote attackers to cause a denial of service (CPU consumption) via a web page that calls the JavaScript setInterval method, which triggers an incompatibility between the WTF::currentTime and base::Time functions.
CVE-2009-3934	The WebFrameLoaderClient::dispatchDidChangeLocationWithinPage function in src/webkit/glue/webframeloaderclient_impl.cc in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service via a page-local link, related to an "empty redirect chain," as demonstrated by a message in Yahoo! Mail.
CVE-2010-0315	WebKit before r53607, as used in Google Chrome before 4.0.249.89, allows remote attackers to discover a redirect's target URL, for the session of a specific user of a web site, by placing the site's URL in the HREF attribute of a stylesheet LINK element, and then reading the document.styleSheets[0].href property value, related to an IFRAME element.
CVE-2010-0556	browser/login/login_prompt.cc in Google Chrome before 4.0.249.89 populates an authentication dialog with credentials that were stored by Password Manager for a different web site, which allows user-assisted remote HTTP servers to obtain sensitive information via a URL that requires authentication, as demonstrated by a URL in the SRC attribute of an IMG element.
CVE-2010-0643	Google Chrome before 4.0.249.89 attempts to make direct connections to web sites when all configured proxy servers are unavailable, which allows remote HTTP servers to obtain potentially sensitive information about the

	identity of a client user via standard HTTP logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.
CVE-2010-0644	Google Chrome before 4.0.249.89, when a SOCKS 5 proxy server is configured, sends DNS queries directly, which allows remote DNS servers to obtain potentially sensitive information about the identity of a client user via request logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.
CVE-2010-0645	Multiple integer overflows in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.
CVE-2010-0646	Multiple integer signedness errors in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.
CVE-2010-0647	WebKit before r53525, as used in Google Chrome before 4.0.249.89, allows remote attackers to execute arbitrary code in the Chrome sandbox via a malformed RUBY element, as demonstrated by a <ruby>><table><rt> sequence.
CVE-2010-0649	Integer overflow in the CrossCallParamsEx::CreateFromBuffer function in sandbox/src/crosscall_server.cc in Google Chrome before 4.0.249.89 allows attackers to leverage renderer access to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a malformed message, related to deserializing of sandbox messages.
CVE-2010-0650	WebKit, as used in Google Chrome before 4.0.249.78 and Apple Safari, allows remote attackers to bypass intended restrictions on popup windows via crafted use of a mouse click event.
CVE-2010-0651	WebKit before r52784, as used in Google Chrome before 4.0.249.78 and Apple Safari before 4.0.5, permits 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-2010-0655	Use-after-free vulnerability in Google Chrome before 4.0.249.78 allows user-assisted remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving the display of a blocked popup window during navigation to a different web site.
CVE-2010-0656	WebKit before r51295, as used in Google Chrome before 4.0.249.78, presents a directory-listing page in response to an XMLHttpRequest for a file:/// URL that corresponds to a directory, which allows attackers to obtain sensitive information or possibly have unspecified other impact via a crafted local HTML document.
CVE-2010-0657	Google Chrome before 4.0.249.78 on Windows does not perform the expected encoding, escaping, and quoting for the URL in the --app argument in a desktop shortcut, which allows user-assisted remote attackers to execute arbitrary programs or obtain sensitive information by tricking a user into creating a crafted shortcut.
CVE-2010-0658	Multiple integer overflows in Skia, as used in Google Chrome before 4.0.249.78, allow remote attackers to execute arbitrary code in the Chrome sandbox or cause a denial of service (memory corruption and application crash) via vectors involving CANVAS elements.
CVE-2010-0659	The image decoder in WebKit before r52833, as used in Google Chrome before 4.0.249.78, does not properly handle a failure of memory allocation, which allows remote attackers to execute arbitrary code in the Chrome sandbox via a malformed GIF file that specifies a large size.
CVE-2010-0660	Google Chrome before 4.0.249.78 sends an https URL in the Referer header of an http request in certain circumstances involving https to http redirection, which allows remote HTTP servers to obtain potentially sensitive information via standard HTTP logging.
CVE-2010-0661	WebCore/bindings/v8/custom/V8DOMWindowCustom.cpp in WebKit before r52401, as used in Google Chrome before 4.0.249.78, allows remote attackers to bypass the Same Origin Policy via vectors involving the window.open method.
CVE-2010-0662	The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome before 4.0.249.78 does not use the correct variables in calculations designed to prevent integer overflows, which allows attackers to leverage renderer access to cause a denial of service or possibly have unspecified other impact via bitmap data, related to deserialization.
CVE-2010-0663	The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome before 4.0.249.78 does not initialize the memory locations that will hold bitmap data, which might allow remote attackers to obtain potentially sensitive information from process memory by providing insufficient data, related to use of a (1) thumbnail database or (2) HTML canvas.
CVE-2010-0664	Stack consumption vulnerability in the ChildProcessSecurityPolicy::CanRequestURL function in browser/child_process_security_policy.cc in Google Chrome before 4.0.249.78 allows remote attackers to cause a denial of service (memory consumption and application crash) via a URL that specifies multiple protocols, as demonstrated by a URL that begins with many repetitions of the view-source: substring.
CVE-2010-1029	Stack consumption vulnerability in the WebCore::CSSSelector function in WebKit, as used in Apple Safari 4.0.4, Apple Safari on iPhone OS and iPhone OS for iPod touch, and Google Chrome 4.0.249, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a STYLE element composed of a large number of *> sequences.
CVE-2010-1228	Multiple race conditions in the sandbox infrastructure in Google Chrome before 4.1.249.1036 have unspecified impact and attack vectors.

CVE-2010-1229	The sandbox infrastructure in Google Chrome before 4.1.249.1036 does not properly use pointers, which has unspecified impact and attack vectors.
CVE-2010-1230	Google Chrome before 4.1.249.1036 does not have the expected behavior for attempts to delete Web SQL Databases and clear the Strict Transport Security (STS) state, which has unspecified impact and attack vectors.
CVE-2010-1231	Google Chrome before 4.1.249.1036 processes HTTP headers before invoking the SafeBrowsing feature, which allows remote attackers to have an unspecified impact via crafted headers.
CVE-2010-1232	Google Chrome before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via a malformed SVG document.
CVE-2010-1233	Multiple integer overflows in Google Chrome before 4.1.249.1036 allow remote attackers to have an unspecified impact via vectors involving WebKit JavaScript objects.
CVE-2010-1234	Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to truncate the URL shown in the HTTP Basic Authentication dialog via unknown vectors.
CVE-2010-1235	Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to trigger the omission of a download warning dialog via unknown vectors.
CVE-2010-1236	The protocolIs function in platform/KURLGoogle.cpp in WebCore in WebKit before r55822, as used in Google Chrome before 4.1.249.1036 and Flock Browser 3.x before 3.0.0.4112, does not properly handle whitespace at the beginning of a URL, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted javascript: URL, as demonstrated by a \x00javascript:alert sequence.
CVE-2010-1237	Google Chrome 4.1 BETA before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via an empty SVG element.
CVE-2010-1500	Google Chrome before 4.1.249.1059 does not properly support forms, which has unknown impact and attack vectors, related to a "type confusion error."
CVE-2010-1502	Unspecified vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to access local files via vectors related to "developer tools."
CVE-2010-1503	Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://net-internals URI.
CVE-2010-1504	Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://downloads URI.
CVE-2010-1505	Google Chrome before 4.1.249.1059 does not prevent pages from loading with the New Tab page's privileges, which has unknown impact and attack vectors.
CVE-2010-1506	The Google V8 bindings in Google Chrome before 4.1.249.1059 allow attackers to cause a denial of service (memory corruption) via unknown vectors.
CVE-2010-1663	The Google URL Parsing Library (aka google-url or GURL) in Google Chrome before 4.1.249.1064 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2010-1664	Google Chrome before 4.1.249.1064 does not properly handle HTML5 media, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.
CVE-2010-1665	Google Chrome before 4.1.249.1064 does not properly handle fonts, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.
CVE-2010-1731	Google Chrome on the HTC Hero allows remote attackers to cause a denial of service (application crash) via JavaScript that writes <marquee> sequences in an infinite loop.
CVE-2010-1767	Cross-site request forgery (CSRF) vulnerability in loader/DocumentThreadableLoader.cpp in WebCore in WebKit before r57041, as used in Google Chrome before 4.1.249.1059, allows remote attackers to hijack the authentication of unspecified victims via a crafted synchronous preflight XMLHttpRequest operation.
CVE-2010-1770	WebKit in Apple Safari before 5.0 on Mac OS X 10.5 through 10.6 and Windows, Apple Safari before 4.1 on Mac OS X 10.4, and Google Chrome before 5.0.375.70 does not properly handle a transformation of a text node that has the IBM1147 character set, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted HTML document containing a BR element, related to a "type checking issue."
CVE-2010-1772	Use-after-free vulnerability in page/Geolocation.cpp in WebCore in WebKit before r59859, as used in Google Chrome before 5.0.375.70, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted web site, related to failure to stop timers associated with geolocation upon deletion of a document.
CVE-2010-1773	Off-by-one error in the toAlphabetic function in rendering/RenderListMarker.cpp in WebCore in WebKit before r59950, as used in Google Chrome before 5.0.375.70, allows remote attackers to obtain sensitive information, cause a denial of service (memory corruption and application crash), or possibly execute arbitrary code via vectors related to list markers for HTML lists, aka rdar problem 8009118.
CVE-2010-1822	WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3 and Google Chrome before 6.0.472.62, does not properly perform a cast of an unspecified variable, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an SVG element in a non-SVG document.
CVE-2010-1823	Use-after-free vulnerability in WebKit before r65958, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger use of

	document APIs such as document.close during parsing, as demonstrated by a Cascading Style Sheets (CSS) file referencing an invalid SVG font, aka rdar problem 8442098.
CVE-2010-1824	Use-after-free vulnerability in WebKit, as used in Apple iTunes before 10.2 on Windows, Apple Safari, and Google Chrome before 6.0.472.59, allows remote attackers to execute arbitrary code or cause a denial of service via vectors related to SVG styles, the DOM tree, and error messages.
CVE-2010-1825	Use-after-free vulnerability in WebKit, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to nested SVG elements.
CVE-2010-1851	Google Chrome, when the Invisible Hand extension is enabled, uses cookies during background HTTP requests in a possibly unexpected manner, which might allow remote web servers to identify specific persons and their product searches via HTTP request logging, related to a "cross-site data leakage" issue.
CVE-2010-1992	Google Chrome 1.0.154.48 executes a mail application in situations where an IFRAME element has a mailto: URL in its SRC attribute, which allows remote attackers to cause a denial of service (excessive application launches) via an HTML document with many IFRAME elements.
CVE-2010-2105	Google Chrome before 5.0.375.55 does not properly follow the Safe Browsing specification's requirements for canonicalization of URLs, which has unspecified impact and remote attack vectors.
CVE-2010-2106	Unspecified vulnerability in Google Chrome before 5.0.375.55 might allow remote attackers to spoof the URL bar via vectors involving unload event handlers.
CVE-2010-2107	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the Safe Browsing functionality.
CVE-2010-2108	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.
CVE-2010-2109	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows user-assisted remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the "drag + drop" functionality.
CVE-2010-2110	Google Chrome before 5.0.375.55 does not properly execute JavaScript code in the extension context, which has unspecified impact and remote attack vectors.
CVE-2010-2120	Google Chrome 1.0.154.48 allows remote attackers to cause a denial of service (resource consumption) via JavaScript code containing an infinite loop that creates IFRAME elements for invalid news:// URIs.
CVE-2010-2179	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, when Firefox or Chrome is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to URL parsing.
CVE-2010-2295	page/EventHandler.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 does not properly handle a change of the focused frame during the dispatching of keydown, which allows user-assisted remote attackers to redirect keystrokes via a crafted HTML document, aka rdar problem 7018610. NOTE: this might overlap CVE-2010-1422.
CVE-2010-2296	The implementation of unspecified DOM methods in Google Chrome before 5.0.375.70 allows remote attackers to bypass the Same Origin Policy via unknown vectors.
CVE-2010-2297	rendering/FixedTableLayout.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an HTML document that has a large colspan attribute within a table.
CVE-2010-2298	browser/renderer_host/database_dispatcher_host.cc in Google Chrome before 5.0.375.70 on Linux does not properly handle ViewHostMsg_DatabaseOpenFile messages in chroot-based sandboxing, which allows remote attackers to bypass intended sandbox restrictions via vectors involving fchdir and chdir calls.
CVE-2010-2299	The Clipboard::DispatchObject function in app/clipboard/clipboard.cc in Google Chrome before 5.0.375.70 does not properly handle CBF_SMBITMAP objects in a ViewHostMsg_ClipboardWriteObjectsAsync message, which might allow remote attackers to execute arbitrary code via vectors involving crafted data from the renderer process, related to a "Type Confusion" issue.
CVE-2010-2300	Use-after-free vulnerability in the Element::normalizeAttributes function in dom/Element.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to handlers for DOM mutation events, aka rdar problem 7948784. NOTE: this might overlap CVE-2010-1759.
CVE-2010-2301	Cross-site scripting (XSS) vulnerability in editing/markup.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to inject arbitrary web script or HTML via vectors related to the node.innerHTML property of a TEXTAREA element. NOTE: this might overlap CVE-2010-1762.
CVE-2010-2302	Use-after-free vulnerability in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via vectors involving remote fonts in conjunction with shadow DOM trees, aka rdar problem 8007953. NOTE: this might overlap CVE-2010-1771.
CVE-2010-2645	Unspecified vulnerability in Google Chrome before 5.0.375.99, when WebGL is used, allows remote attackers to cause a denial of service (out-of-bounds read) via unknown vectors.
CVE-2010-2646	Google Chrome before 5.0.375.99 does not properly isolate sandboxed IFRAME elements, which has unspecified impact and remote attack vectors.

CVE-2010-2647	Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an invalid SVG document.
CVE-2010-2648	The implementation of the Unicode Bidirectional Algorithm (aka Bidi algorithm or UBA) in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2649	Unspecified vulnerability in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (application crash) via an invalid image.
CVE-2010-2650	Unspecified vulnerability in Google Chrome before 5.0.375.99 has unknown impact and attack vectors, related to an "annoyance with print dialogs."
CVE-2010-2651	The Cascading Style Sheets (CSS) implementation in Google Chrome before 5.0.375.99 does not properly perform style rendering, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2652	Google Chrome before 5.0.375.99 does not properly implement modal dialogs, which allows attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-2897	Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the Windows kernel, which has unknown impact and attack vectors.
CVE-2010-2898	Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the GNU C Library, which has unknown impact and attack vectors.
CVE-2010-2899	Unspecified vulnerability in the layout implementation in Google Chrome before 5.0.375.125 allows remote attackers to obtain sensitive information from process memory via unknown vectors.
CVE-2010-2900	Google Chrome before 5.0.375.125 does not properly handle a large canvas, which has unspecified impact and remote attack vectors.
CVE-2010-2901	The rendering implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2902	The SVG implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2903	Google Chrome before 5.0.375.125 performs unexpected truncation and improper eliding of hostnames, which has unspecified impact and remote attack vectors.
CVE-2010-3111	Google Chrome before 6.0.472.53 does not properly mitigate an unspecified flaw in the Windows kernel, which has unknown impact and attack vectors, a different vulnerability than CVE-2010-2897.
CVE-2010-3112	Google Chrome before 5.0.375.127 does not properly implement file dialogs, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3113	Google Chrome before 5.0.375.127, and webkitgtk before 1.2.5, does not properly handle SVG documents, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors related to state changes when using DeleteButtonController.
CVE-2010-3114	The text-editing implementation in Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not check a node type before performing a cast, which has unspecified impact and attack vectors related to (1) DeleteSelectionCommand.cpp, (2) InsertLineBreakCommand.cpp, or (3) InsertParagraphSeparatorCommand.cpp in WebCore/editing/.
CVE-2010-3115	Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not properly implement the history feature, which might allow remote attackers to spoof the address bar via unspecified vectors.
CVE-2010-3116	Multiple use-after-free vulnerabilities in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors related to improper handling of MIME types by plug-ins.
CVE-2010-3117	Google Chrome before 5.0.375.127 does not properly implement the notifications feature, which allows remote attackers to cause a denial of service (application crash) and possibly have unspecified other impact via unknown vectors.
CVE-2010-3118	The autosuggest feature in the Omnibox implementation in Google Chrome before 5.0.375.127 does not anticipate entry of passwords, which might allow remote attackers to obtain sensitive information by reading the network traffic generated by this feature.
CVE-2010-3119	Google Chrome before 5.0.375.127 and webkitgtk before 1.2.6 do not properly support the Ruby language, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3120	Google Chrome before 5.0.375.127 does not properly implement the Geolocation feature, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3246	Google Chrome before 6.0.472.53 does not properly handle the _blank value for the target attribute of unspecified elements, which allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-3247	Google Chrome before 6.0.472.53 does not properly restrict the characters in URLs, which allows remote attackers to spoof the appearance of the URL bar via homographic sequences.

CVE-2010-3248	Google Chrome before 6.0.472.53 does not properly restrict copying to the clipboard, which has unspecified impact and attack vectors.
CVE-2010-3249	Google Chrome before 6.0.472.53 does not properly implement SVG filters, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "stale pointer" issue.
CVE-2010-3250	Unspecified vulnerability in Google Chrome before 6.0.472.53 allows remote attackers to enumerate the set of installed extensions via unknown vectors.
CVE-2010-3251	The WebSockets implementation in Google Chrome before 6.0.472.53 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.
CVE-2010-3252	Use-after-free vulnerability in the Notifications presenter in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-3253	The implementation of notification permissions in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3254	The WebSockets implementation in Google Chrome before 6.0.472.53 does not properly handle integer values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-3255	Google Chrome before 6.0.472.53 and webkitgtk before 1.2.6 do not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3256	Google Chrome before 6.0.472.53 does not properly limit the number of stored autocomplete entries, which has unspecified impact and attack vectors.
CVE-2010-3257	Use-after-free vulnerability in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 6.0.472.53, and webkitgtk before 1.2.6, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving element focus.
CVE-2010-3258	The sandbox implementation in Google Chrome before 6.0.472.53 does not properly deserialize parameters, which has unspecified impact and remote attack vectors.
CVE-2010-3259	WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 6.0.472.53, and webkitgtk before 1.2.6, does not properly restrict read access to images derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive image data via a crafted web site.
CVE-2010-3411	Google Chrome before 6.0.472.59 on Linux does not properly handle cursors, which might allow attackers to cause a denial of service (assertion failure) via unspecified vectors.
CVE-2010-3412	Race condition in the console implementation in Google Chrome before 6.0.472.59 has unspecified impact and attack vectors.
CVE-2010-3413	Unspecified vulnerability in the pop-up blocking functionality in Google Chrome before 6.0.472.59 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2010-3414	Google Chrome before 6.0.472.59 on Mac OS X does not properly implement file dialogs, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. NOTE: this issue exists because of an incorrect fix for CVE-2010-3112 on Mac OS X.
CVE-2010-3415	Google Chrome before 6.0.472.59 does not properly implement Geolocation, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3416	Google Chrome before 6.0.472.59 on Linux does not properly implement the Khmer locale, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3417	Google Chrome before 6.0.472.59 does not prompt the user before granting access to the extension history, which allows attackers to obtain potentially sensitive information via unspecified vectors.
CVE-2010-3729	The SPDY protocol implementation in Google Chrome before 6.0.472.62 does not properly manage buffers, which might allow remote attackers to execute arbitrary code via unspecified vectors.
CVE-2010-3730	Google Chrome before 6.0.472.62 does not properly use information about the origin of a document to manage properties, which allows remote attackers to have an unspecified impact via a crafted web site, related to a "property pollution" issue.
CVE-2010-4008	libxml2 before 2.7.8, as used in Google Chrome before 7.0.517.44, Apple Safari 5.0.2 and earlier, and other products, reads from invalid memory locations during processing of malformed XPath expressions, which allows context-dependent attackers to cause a denial of service (application crash) via a crafted XML document.
CVE-2010-4033	Google Chrome before 7.0.517.41 does not properly implement the autofill and autocomplete functionality, which allows remote attackers to conduct "profile spamming" attacks via unspecified vectors.
CVE-2010-4034	Google Chrome before 7.0.517.41 does not properly handle forms, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4035	Google Chrome before 7.0.517.41 does not properly perform autofill operations for forms, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.

CVE-2010-4036	Google Chrome before 7.0.517.41 does not properly handle the unloading of a page, which allows remote attackers to spoof URLs via unspecified vectors.
CVE-2010-4037	Unspecified vulnerability in Google Chrome before 7.0.517.41 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-4038	The Web Sockets implementation in Google Chrome before 7.0.517.41 does not properly handle a shutdown action, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4039	Google Chrome before 7.0.517.41 on Linux does not properly set the PATH environment variable, which has unspecified impact and attack vectors.
CVE-2010-4040	Google Chrome before 7.0.517.41 does not properly handle animated GIF images, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted image.
CVE-2010-4041	The sandbox implementation in Google Chrome before 7.0.517.41 on Linux does not properly constrain worker processes, which might allow remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2010-4042	Google Chrome before 7.0.517.41 does not properly handle element maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "stale elements."
CVE-2010-4197	Use-after-free vulnerability in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text editing.
CVE-2010-4198	WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, does not properly handle large text areas, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4199	Google Chrome before 7.0.517.44 does not properly perform a cast of an unspecified variable during processing of an SVG use element, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SVG document.
CVE-2010-4201	Use-after-free vulnerability in Google Chrome before 7.0.517.44 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text control selections.
CVE-2010-4202	Multiple integer overflows in Google Chrome before 7.0.517.44 on Linux allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted font.
CVE-2010-4203	WebM libvpx (aka the VP8 Codec SDK) before 0.9.5, as used in Google Chrome before 7.0.517.44, allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via invalid frames.
CVE-2010-4204	WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, accesses a frame object after this object has been destroyed, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-4205	Google Chrome before 7.0.517.44 does not properly handle the data types of event objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-4206	Array index error in the FEBBlend::apply function in WebCore/platform/graphics/filters/FEBBlend.cpp in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted SVG document, related to effects in the application of filters.
CVE-2010-4482	Unspecified vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-4483	Google Chrome before 8.0.552.215 does not properly restrict read access to videos derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive video data via a crafted web site.
CVE-2010-4484	Google Chrome before 8.0.552.215 does not properly handle HTML5 databases, which allows attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4485	Google Chrome before 8.0.552.215 does not properly restrict the generation of file dialogs, which allows remote attackers to cause a denial of service (reduced usability and possible application crash) via a crafted web site.
CVE-2010-4486	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to history handling.
CVE-2010-4487	Incomplete blacklist vulnerability in Google Chrome before 8.0.552.215 on Linux and Mac OS X allows remote attackers to have an unspecified impact via a "dangerous file."
CVE-2010-4488	Google Chrome before 8.0.552.215 does not properly handle HTTP proxy authentication, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4489	libvpx, as used in Google Chrome before 8.0.552.215 and possibly other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebM video. NOTE: this vulnerability exists because of a regression.
CVE-2010-4490	Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via malformed video content that triggers an indexing error.
CVE-2010-4491	Google Chrome before 8.0.552.215 does not properly restrict privileged extensions, which allows remote attackers to cause a denial of service (memory corruption) via a crafted extension.

CVE-2010-4492	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animations.
CVE-2010-4493	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service via vectors related to the handling of mouse dragging events.
CVE-2010-4494	Double free vulnerability in libxml2 2.7.8 and other versions, as used in Google Chrome before 8.0.552.215 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.
CVE-2010-4574	The Pickle::Pickle function in base/pickle.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 on 64-bit Linux platforms does not properly perform pointer arithmetic, which allows remote attackers to bypass message deserialization validation, and cause a denial of service or possibly have unspecified other impact, via invalid pickle data.
CVE-2010-4575	The ThemeInstalledInfoBarDelegate::Observe function in browser/extensions/theme_installed_infobar_delegate.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle incorrect tab interaction by an extension, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted extension.
CVE-2010-4576	browser/worker_host/message_port_dispatcher.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle certain postMessage calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code that creates a web worker.
CVE-2010-4577	The CSSParser::parseFontFaceSrc function in WebCore/css/CSSParser.cpp in WebKit, as used in Google Chrome before 8.0.552.224, Chrome OS before 8.0.552.343, webkitgtk before 1.2.6, and other products does not properly parse Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted local font, related to "Type Confusion."
CVE-2010-4578	Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 do not properly perform cursor handling, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2010-5069	The Cascading Style Sheets (CSS) implementation in Google Chrome 4 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. NOTE: this may overlap CVE-2010-2264.
CVE-2010-5073	The JavaScript implementation in Google Chrome 4 does not properly restrict the set of values contained in the object returned by the getComputedStyle method, which allows remote attackers to obtain sensitive information about visited web pages by calling this method. NOTE: this may overlap CVE-2010-5070.
CVE-2011-0470	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle extensions notification, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-0471	The node-iteration implementation in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 does not properly handle pointers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-0472	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle the printing of PDF documents, which allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a multi-page document.
CVE-2011-0473	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with CANVAS elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0474	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0475	Use-after-free vulnerability in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a PDF document.
CVE-2011-0476	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allow remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via a PDF document that triggers an out-of-memory error.
CVE-2011-0477	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle a mismatch in video frame sizes, which allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via unknown vectors.
CVE-2011-0478	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle SVG use elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0479	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly interact with extensions, which allows remote attackers to cause a denial of service via a crafted extension that triggers an uninitialized pointer.
CVE-2011-0480	Multiple buffer overflows in vorbis_dec.c in the Vorbis decoder in FFmpeg, as used in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344, allow remote attackers to cause a denial of service (memory

	corruption and application crash) or possibly have unspecified other impact via a crafted WebM file, related to buffers for (1) the channel floor and (2) the channel residue.
CVE-2011-0481	Buffer overflow in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF shading.
CVE-2011-0482	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of anchors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-0483	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of video, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-0484	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform DOM node removal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale rendering node."
CVE-2011-0485	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle speech data, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to a "stale pointer."
CVE-2011-0776	The sandbox implementation in Google Chrome before 9.0.597.84 on Mac OS X might allow remote attackers to obtain potentially sensitive information about local files via vectors related to the stat system call.
CVE-2011-0777	Use-after-free vulnerability in Google Chrome before 9.0.597.84 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to image loading.
CVE-2011-0778	Google Chrome before 9.0.597.84 does not properly restrict drag and drop operations, which might allow remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-0779	Google Chrome before 9.0.597.84 does not properly handle a missing key in an extension, which allows remote attackers to cause a denial of service (application crash) via a crafted extension.
CVE-2011-0780	The PDF event handler in Google Chrome before 9.0.597.84 does not properly interact with print operations, which allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-0781	Google Chrome before 9.0.597.84 does not properly handle autofill profile merging, which has unspecified impact and remote attack vectors.
CVE-2011-0782	Google Chrome before 9.0.597.84 on Mac OS X does not properly mitigate an unspecified flaw in the Mac OS X 10.5 SSL libraries, which allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2011-0783	Unspecified vulnerability in Google Chrome before 9.0.597.84 allows user-assisted remote attackers to cause a denial of service (application crash) via vectors involving a "bad volume setting."
CVE-2011-0784	Race condition in Google Chrome before 9.0.597.84 allows remote attackers to execute arbitrary code via vectors related to audio.
CVE-2011-0981	Google Chrome before 9.0.597.94 does not properly perform event handling for animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0982	Use-after-free vulnerability in Google Chrome before 9.0.597.94 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG font faces.
CVE-2011-0983	Google Chrome before 9.0.597.94 does not properly handle anonymous blocks, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0984	Google Chrome before 9.0.597.94 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-0985	Google Chrome before 9.0.597.94 does not properly perform process termination upon memory exhaustion, which has unspecified impact and remote attack vectors.
CVE-2011-1059	Use-after-free vulnerability in WebCore in WebKit before r77705, as used in Google Chrome before 11.0.672.2 and other products, allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that entice a user to resubmit a form, related to improper handling of provisional items by the HistoryController component, aka rdar problem 8938557.
CVE-2011-1107	Unspecified vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to spoof the URL bar via unknown vectors.
CVE-2011-1108	Google Chrome before 9.0.597.107 does not properly implement JavaScript dialogs, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1109	Google Chrome before 9.0.597.107 does not properly process nodes in Cascading Style Sheets (CSS) stylesheets, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."

CVE-2011-1110	Google Chrome before 9.0.597.107 does not properly implement key frame rules, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1111	Google Chrome before 9.0.597.107 does not properly implement forms controls, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1112	Google Chrome before 9.0.597.107 does not properly perform SVG rendering, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1113	Google Chrome before 9.0.597.107 on 64-bit Linux platforms does not properly perform pickle serialization, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1114	Google Chrome before 9.0.597.107 does not properly handle tables, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-1115	Google Chrome before 9.0.597.107 does not properly render tables, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1116	Google Chrome before 9.0.597.107 does not properly handle SVG animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1117	Google Chrome before 9.0.597.107 does not properly handle XHTML documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale nodes."
CVE-2011-1118	Google Chrome before 9.0.597.107 does not properly handle TEXTAREA elements, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1119	Google Chrome before 9.0.597.107 does not properly determine device orientation, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1120	The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, aka Issue 71717.
CVE-2011-1121	Integer overflow in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a TEXTAREA element.
CVE-2011-1122	The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, aka Issue 71960.
CVE-2011-1123	Google Chrome before 9.0.597.107 does not properly restrict access to internal extension functions, which has unspecified impact and remote attack vectors.
CVE-2011-1124	Use-after-free vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to blocked plug-ins.
CVE-2011-1125	Google Chrome before 9.0.597.107 does not properly perform layout, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1185	Google Chrome before 10.0.648.127 does not prevent (1) navigation and (2) close operations on the top location of a sandboxed frame, which has unspecified impact and remote attack vectors.
CVE-2011-1186	Google Chrome before 10.0.648.127 on Linux does not properly handle parallel execution of calls to the print method, which might allow remote attackers to cause a denial of service (application crash) via crafted JavaScript code.
CVE-2011-1187	Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."
CVE-2011-1188	Google Chrome before 10.0.648.127 does not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1189	Google Chrome before 10.0.648.127 does not properly perform box layout, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-1190	The Web Workers implementation in Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."
CVE-2011-1191	Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of DOM URLs.
CVE-2011-1192	Google Chrome before 10.0.648.127 on Linux does not properly handle Unicode ranges, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1193	Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-1194	Multiple unspecified vulnerabilities in Google Chrome before 10.0.648.127 allow remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2011-1195	Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "document script lifetime handling."
CVE-2011-1196	The OGG container implementation in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.

CVE-2011-1197	Google Chrome before 10.0.648.127 does not properly perform table painting, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1198	The video functionality in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger use of a malformed "out-of-bounds structure."
CVE-2011-1199	Google Chrome before 10.0.648.127 does not properly handle DataView objects, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1200	Google Chrome before 10.0.648.127 does not properly perform a cast of an unspecified variable during text rendering, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-1201	The context implementation in WebKit, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1202	The xsltGenerateIdFunction function in functions.c in libxslt 1.1.26 and earlier, as used in Google Chrome before 10.0.648.127 and other products, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function.
CVE-2011-1203	Google Chrome before 10.0.648.127 does not properly handle SVG cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1204	Google Chrome before 10.0.648.127 does not properly handle attributes, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via a crafted document.
CVE-2011-1285	The regular-expression functionality in Google Chrome before 10.0.648.127 does not properly implement reentrancy, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1286	Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger incorrect access to memory.
CVE-2011-1291	Google Chrome before 10.0.648.204 does not properly handle base strings, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "buffer error."
CVE-2011-1292	Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1293	Use-after-free vulnerability in the HTMLCollection implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1294	Google Chrome before 10.0.648.204 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1295	WebKit, as used in Google Chrome before 10.0.648.204 and Apple Safari before 5.0.6, does not properly handle node parentage, which allows remote attackers to cause a denial of service (DOM tree corruption), conduct cross-site scripting (XSS) attacks, or possibly have unspecified other impact via unknown vectors.
CVE-2011-1296	Google Chrome before 10.0.648.204 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1300	The Program::getActiveUniformMaxLength function in libGLESv2/Program.cpp in libGLESv2.dll in the WebGLES library in Almost Native Graphics Layer Engine (ANGLE), as used in Mozilla Firefox 4.x before 4.0.1 on Windows and in the GPU process in Google Chrome before 10.0.648.205 on Windows, allows remote attackers to execute arbitrary code via unspecified vectors, related to an "off-by-three" error.
CVE-2011-1301	Use-after-free vulnerability in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.
CVE-2011-1302	Heap-based buffer overflow in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.
CVE-2011-1303	Google Chrome before 11.0.696.57 does not properly handle floating objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1304	Unspecified vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to bypass the pop-up blocker via vectors related to plug-ins.
CVE-2011-1305	Race condition in Google Chrome before 11.0.696.57 on Linux and Mac OS X allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to linked lists and a database.
CVE-2011-1413	Google Chrome before 10.0.648.127 on Linux does not properly mitigate an unspecified flaw in an X server, which allows remote attackers to cause a denial of service (application crash) via vectors involving long messages.
CVE-2011-1434	Google Chrome before 11.0.696.57 does not ensure thread safety during handling of MIME data, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1435	Google Chrome before 11.0.696.57 does not properly implement the tabs permission for extensions, which allows remote attackers to read local files via a crafted extension.

CVE-2011-1436	Google Chrome before 11.0.696.57 on Linux does not properly interact with the X Window System, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-1437	Multiple integer overflows in Google Chrome before 11.0.696.57 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float rendering.
CVE-2011-1438	Google Chrome before 11.0.696.57 allows remote attackers to bypass the Same Origin Policy via vectors involving blobs.
CVE-2011-1439	Google Chrome before 11.0.696.57 on Linux does not properly isolate renderer processes, which has unspecified impact and remote attack vectors.
CVE-2011-1440	Use-after-free vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the ruby element and Cascading Style Sheets (CSS) token sequences.
CVE-2011-1441	Google Chrome before 11.0.696.57 does not properly perform a cast of an unspecified variable during handling of floating select lists, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document.
CVE-2011-1442	Google Chrome before 11.0.696.57 does not properly handle mutation events, which allows remote attackers to cause a denial of service (node tree corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1443	Google Chrome before 11.0.696.57 does not properly implement layering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2011-1444	Race condition in the sandbox launcher implementation in Google Chrome before 11.0.696.57 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1445	Google Chrome before 11.0.696.57 does not properly handle SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1446	Google Chrome before 11.0.696.57 allows remote attackers to spoof the URL bar via vectors involving (1) a navigation error or (2) an interrupted load.
CVE-2011-1447	Google Chrome before 11.0.696.57 does not properly handle drop-down lists, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1448	Google Chrome before 11.0.696.57 does not properly perform height calculations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1449	Use-after-free vulnerability in the WebSockets implementation in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1450	Google Chrome before 11.0.696.57 does not properly present file dialogs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."
CVE-2011-1451	Google Chrome before 11.0.696.57 does not properly handle DOM id maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."
CVE-2011-1452	Google Chrome before 11.0.696.57 allows user-assisted remote attackers to spoof the URL bar via vectors involving a redirect and a manual reload.
CVE-2011-1454	Use-after-free vulnerability in the DOM id handling functionality in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1455	Google Chrome before 11.0.696.57 does not properly handle PDF documents with multipart encoding, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2011-1456	Google Chrome before 11.0.696.57 does not properly handle PDF forms, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2011-1465	The SPDY implementation in net/http/http_network_transaction.cc in Google Chrome before 11.0.696.14 drains the bodies from SPDY responses, which might allow remote SPDY servers to cause a denial of service (application exit) by canceling a stream.
CVE-2011-1691	The counterToCSSValue function in CSSComputedStyleDeclaration.cpp in the Cascading Style Sheets (CSS) implementation in WebCore in WebKit before r82222, as used in Google Chrome before 11.0.696.43 and other products, does not properly handle access to the (1) counterIncrement and (2) counterReset attributes of CSSStyleDeclaration data provided by a getComputedStyle method call, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code.
CVE-2011-1793	rendering/svg/RenderSVGResourceFilter.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted SVG document that leads to a "stale pointer."
CVE-2011-1794	Integer overflow in the FilterEffect::copyImageBytes function in platform/graphics/filters/FilterEffect.cpp in the SVG filter implementation in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted dimensions.
CVE-2011-1795	Integer underflow in the HTMLFormElement::removeFormElement function in html/HTMLFormElement.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service

	(application crash) or possibly have unspecified other impact via a crafted HTML document containing a FORM element.
CVE-2011-1796	Use-after-free vulnerability in the FrameView::calculateScrollbarModesForLayout function in page/FrameView.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that calls the removeChild method during interaction with a FRAME element.
CVE-2011-1798	rendering/svg/RenderSVGText.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 does not properly perform a cast of an unspecified variable during an attempt to handle a block child, which allows remote attackers to cause a denial of service (application crash) or possibly have unknown other impact via a crafted text element in an SVG document.
CVE-2011-1799	Google Chrome before 11.0.696.68 does not properly perform casts of variables during interaction with the WebKit engine, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1800	Multiple integer overflows in the SVG Filters implementation in WebCore in WebKit in Google Chrome before 11.0.696.68 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1801	Unspecified vulnerability in Google Chrome before 11.0.696.71 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2011-1804	rendering/RenderBox.cpp in WebCore in WebKit before r86862, as used in Google Chrome before 11.0.696.71, does not properly render floats, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1806	Google Chrome before 11.0.696.71 does not properly implement the GPU command buffer, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-1807	Google Chrome before 11.0.696.71 does not properly handle blobs, which allows remote attackers to execute arbitrary code via unspecified vectors that trigger an out-of-bounds write.
CVE-2011-1808	Use-after-free vulnerability in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to incorrect integer calculations during float handling.
CVE-2011-1809	Use-after-free vulnerability in the accessibility feature in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1810	The Cascading Style Sheets (CSS) implementation in Google Chrome before 12.0.742.91 does not properly restrict access to the visit history, which allows remote attackers to obtain sensitive information via unspecified vectors.
CVE-2011-1811	Google Chrome before 12.0.742.91 does not properly handle a large number of form submissions, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-1812	Google Chrome before 12.0.742.91 allows remote attackers to bypass intended access restrictions via vectors related to extensions.
CVE-2011-1813	Google Chrome before 12.0.742.91 does not properly implement the framework for extensions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1814	Google Chrome before 12.0.742.91 attempts to read data from an uninitialized pointer, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1815	Google Chrome before 12.0.742.91 allows remote attackers to inject script into a tab page via vectors related to extensions.
CVE-2011-1816	Use-after-free vulnerability in the developer tools in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1817	Google Chrome before 12.0.742.91 does not properly implement history deletion, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1818	Use-after-free vulnerability in the image loader in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1819	Google Chrome before 12.0.742.91 allows remote attackers to perform unspecified injection into a chrome:// page via vectors related to extensions.
CVE-2011-2075	Unspecified vulnerability in Google Chrome 11.0.696.65 on Windows 7 SP1 allows remote attackers to execute arbitrary code via unknown vectors. NOTE: as of 20110510, the only disclosure is a vague advisory that possibly relates to multiple vulnerabilities or multiple products. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.
CVE-2011-2332	Google V8, as used in Google Chrome before 12.0.742.91, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2342	The DOM implementation in Google Chrome before 12.0.742.91 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2345	The NPAPI implementation in Google Chrome before 12.0.742.112 does not properly handle strings, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-2346	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG fonts.
CVE-2011-2347	Google Chrome before 12.0.742.112 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-2348	Google V8, as used in Google Chrome before 12.0.742.112, performs an incorrect bounds check, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2349	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text selection.
CVE-2011-2350	The HTML parser in Google Chrome before 12.0.742.112 does not properly address "lifetime and re-entrancy issues," which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2351	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.
CVE-2011-2358	Google Chrome before 13.0.782.107 does not ensure that extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.
CVE-2011-2359	Google Chrome before 13.0.782.107 does not properly track line boxes during rendering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-2360	Google Chrome before 13.0.782.107 does not ensure that the user is prompted before download of a dangerous file, which makes it easier for remote attackers to bypass intended content restrictions via a crafted web site.
CVE-2011-2361	The Basic Authentication dialog implementation in Google Chrome before 13.0.782.107 does not properly handle strings, which might make it easier for remote attackers to capture credentials via a crafted web site.
CVE-2011-2599	Google Chrome 11 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-2011-2761	Google Chrome 14.0.794.0 does not properly handle a reload of a page generated in response to a POST, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted web site, related to GetWidget methods.
CVE-2011-2782	The drag-and-drop implementation in Google Chrome before 13.0.782.107 on Linux does not properly enforce permissions for files, which allows user-assisted remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2011-2783	Google Chrome before 13.0.782.107 does not ensure that developer-mode NPAPI extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.
CVE-2011-2784	Google Chrome before 13.0.782.107 allows remote attackers to obtain sensitive information via a request for the GL program log, which reveals a local path in an unspecified log entry.
CVE-2011-2785	The extensions implementation in Google Chrome before 13.0.782.107 does not properly validate the URL for the home page, which allows remote attackers to have an unspecified impact via a crafted extension.
CVE-2011-2786	Google Chrome before 13.0.782.107 does not ensure that the speech-input bubble is shown on the product's screen, which might make it easier for remote attackers to make audio recordings via a crafted web page containing an INPUT element.
CVE-2011-2787	Google Chrome before 13.0.782.107 does not properly address re-entrancy issues associated with the GPU lock, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-2788	Buffer overflow in the inspector serialization functionality in Google Chrome before 13.0.782.107 allows user-assisted remote attackers to have an unspecified impact via unknown vectors.
CVE-2011-2789	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to instantiation of the Pepper plug-in.
CVE-2011-2790	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving floating styles.
CVE-2011-2791	The International Components for Unicode (ICU) functionality in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-2792	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float removal.
CVE-2011-2793	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media selectors.
CVE-2011-2794	Google Chrome before 13.0.782.107 does not properly perform text iteration, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2795	Google Chrome before 13.0.782.107 does not prevent calls to functions in other frames, which allows remote attackers to bypass intended access restrictions via a crafted web site, related to a "cross-frame function leak."

CVE-2011-2796	Use-after-free vulnerability in Skia, as used in Google Chrome before 13.0.782.107, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2797	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to resource caching.
CVE-2011-2798	Google Chrome before 13.0.782.107 does not properly restrict access to internal schemes, which allows remote attackers to have an unspecified impact via a crafted web site.
CVE-2011-2799	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to HTML range handling.
CVE-2011-2800	Google Chrome before 13.0.782.107 allows remote attackers to obtain potentially sensitive information about client-side redirect targets via a crafted web site.
CVE-2011-2801	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the frame loader.
CVE-2011-2802	Google V8, as used in Google Chrome before 13.0.782.107, does not properly perform const lookups, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted web site.
CVE-2011-2803	Google Chrome before 13.0.782.107 does not properly handle Skia paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2804	Google Chrome before 13.0.782.107 does not properly handle nested functions in PDF documents, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted document.
CVE-2011-2805	Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy and conduct script injection attacks via unspecified vectors.
CVE-2011-2806	Google Chrome before 13.0.782.215 on Windows does not properly handle vertex data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-2818	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to display box rendering.
CVE-2011-2819	Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy via vectors related to handling of the base URI.
CVE-2011-2821	Double free vulnerability in libxml2, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted XPath expression.
CVE-2011-2822	Google Chrome before 13.0.782.215 on Windows does not properly parse URLs located on the command line, which has unspecified impact and attack vectors.
CVE-2011-2823	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a line box.
CVE-2011-2824	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes.
CVE-2011-2825	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving custom fonts.
CVE-2011-2826	Google Chrome before 13.0.782.215 allows remote attackers to bypass the Same Origin Policy via vectors related to empty origins.
CVE-2011-2827	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text searching.
CVE-2011-2828	Google V8, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-2829	Integer overflow in Google Chrome before 13.0.782.215 on 32-bit platforms allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving uniform arrays.
CVE-2011-2830	Google V8, as used in Google Chrome before 14.0.835.163, does not properly implement script object wrappers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-2834	Double free vulnerability in libxml2, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.
CVE-2011-2835	Race condition in Google Chrome before 14.0.835.163 allows attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the certificate cache.
CVE-2011-2836	Google Chrome before 14.0.835.163 does not require Infobar interaction before use of the Windows Media Player plug-in, which makes it easier for remote attackers to have an unspecified impact via crafted Flash content.
CVE-2011-2837	Google Chrome before 14.0.835.163 on Linux does not use the PIC and PIE compiler options for position-independent code, which has unspecified impact and attack vectors.
CVE-2011-2838	Google Chrome before 14.0.835.163 does not properly consider the MIME type during the loading of a plug-in, which has unspecified impact and remote attack vectors.

CVE-2011-2839	The PDF implementation in Google Chrome before 13.0.782.215 on Linux does not properly use the memset library function, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2840	Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to "unusual user interaction."
CVE-2011-2841	Google Chrome before 14.0.835.163 does not properly perform garbage collection during the processing of PDF documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-2842	The installer in Google Chrome before 14.0.835.163 on Mac OS X does not properly handle lock files, which has unspecified impact and attack vectors.
CVE-2011-2843	Google Chrome before 14.0.835.163 does not properly handle media buffers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2844	Google Chrome before 14.0.835.163 does not properly process MP3 files, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2845	Google Chrome before 15.0.874.102 does not properly handle history data, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-2846	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to unload event handling.
CVE-2011-2847	Use-after-free vulnerability in the document loader in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-2848	Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to the forward button.
CVE-2011-2849	The WebSockets implementation in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.
CVE-2011-2850	Google Chrome before 14.0.835.163 does not properly handle Khmer characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2851	Google Chrome before 14.0.835.163 does not properly handle video, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2852	Off-by-one error in Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2853	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.
CVE-2011-2854	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "ruby / table style handing."
CVE-2011-2855	Google Chrome before 14.0.835.163 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-2856	Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2857	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the focus controller.
CVE-2011-2858	Google Chrome before 14.0.835.163 does not properly handle triangle arrays, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2859	Google Chrome before 14.0.835.163 uses incorrect permissions for non-gallery pages, which has unspecified impact and attack vectors.
CVE-2011-2860	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to table styles.
CVE-2011-2861	Google Chrome before 14.0.835.163 does not properly handle strings in PDF documents, which allows remote attackers to have an unspecified impact via a crafted document that triggers an incorrect read operation.
CVE-2011-2862	Google V8, as used in Google Chrome before 14.0.835.163, does not properly restrict access to built-in objects, which has unspecified impact and remote attack vectors.
CVE-2011-2864	Google Chrome before 14.0.835.163 does not properly handle Tibetan characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2874	Google Chrome before 14.0.835.163 does not perform an expected pin operation for a self-signed certificate during a session, which has unspecified impact and remote attack vectors.
CVE-2011-2875	Google V8, as used in Google Chrome before 14.0.835.163, does not properly perform object sealing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2011-2876	Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a text line box.

CVE-2011-2877	Google Chrome before 14.0.835.202 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale font."
CVE-2011-2878	Google Chrome before 14.0.835.202 does not properly restrict access to the window prototype, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2879	Google Chrome before 14.0.835.202 does not properly consider object lifetimes and thread safety during the handling of audio nodes, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2880	Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.
CVE-2011-2881	Google Chrome before 14.0.835.202 does not properly handle Google V8 hidden objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2011-3015	Multiple integer overflows in the PDF codecs in Google Chrome before 17.0.963.56 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3016	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes, related to a "read-after-free" issue.
CVE-2011-3017	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to database handling.
CVE-2011-3018	Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to path rendering.
CVE-2011-3019	Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska video (aka MKV) file.
CVE-2011-3020	Unspecified vulnerability in the Native Client validator implementation in Google Chrome before 17.0.963.56 has unknown impact and remote attack vectors.
CVE-2011-3021	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to subframe loading.
CVE-2011-3022	translate/translate_manager.cc in Google Chrome before 17.0.963.56 and 19.x before 19.0.1036.7 uses an HTTP session to exchange data for translation, which allows remote attackers to obtain sensitive information by sniffing the network.
CVE-2011-3023	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to drag-and-drop operations.
CVE-2011-3024	Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service (application crash) via an empty X.509 certificate.
CVE-2011-3025	Google Chrome before 17.0.963.56 does not properly parse H.264 data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3026	Integer overflow in libpng, as used in Google Chrome before 17.0.963.56, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an integer truncation.
CVE-2011-3027	Google Chrome before 17.0.963.56 does not properly perform a cast of an unspecified variable during handling of columns, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3031	Use-after-free vulnerability in the element wrapper in Google V8, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3032	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG values.
CVE-2011-3033	Buffer overflow in Skia, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3034	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG document.
CVE-2011-3035	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.
CVE-2011-3036	Google Chrome before 17.0.963.65 does not properly perform a cast of an unspecified variable during handling of line boxes, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3037	Google Chrome before 17.0.963.65 does not properly perform casts of unspecified variables during the splitting of anonymous blocks, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3038	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to multi-column handling.
CVE-2011-3039	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to quote handling.

CVE-2011-3040	Google Chrome before 17.0.963.65 does not properly handle text, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2011-3041	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of class attributes.
CVE-2011-3042	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of table sections.
CVE-2011-3043	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a flexbox (aka flexible box) in conjunction with the floating of elements.
CVE-2011-3044	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animation elements.
CVE-2011-3045	Integer signedness error in the png_inflate function in pngutil.c in libpng before 1.4.10beta01, as used in Google Chrome before 17.0.963.83 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file, a different vulnerability than CVE-2011-3026.
CVE-2011-3046	The extension subsystem in Google Chrome before 17.0.963.78 does not properly handle history navigation, which allows remote attackers to execute arbitrary code by leveraging a "Universal XSS (UXSS)" issue.
CVE-2011-3047	The GPU process in Google Chrome before 17.0.963.79 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) by leveraging an error in the plug-in loading mechanism.
CVE-2011-3049	Google Chrome before 17.0.963.83 does not properly restrict the extension web request API, which allows remote attackers to cause a denial of service (disrupted system requests) via a crafted extension.
CVE-2011-3050	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2011-3051	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the cross-fade function.
CVE-2011-3052	The WebGL implementation in Google Chrome before 17.0.963.83 does not properly handle CANVAS elements, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3053	Use-after-free vulnerability in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to block splitting.
CVE-2011-3054	The WebUI privilege implementation in Google Chrome before 17.0.963.83 does not properly perform isolation, which allows remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2011-3055	The browser native UI in Google Chrome before 17.0.963.83 does not require user confirmation before an unpacked extension installation, which allows user-assisted remote attackers to have an unspecified impact via a crafted extension.
CVE-2011-3056	Google Chrome before 17.0.963.83 allows remote attackers to bypass the Same Origin Policy via vectors involving a "magic iframe."
CVE-2011-3057	Google V8, as used in Google Chrome before 17.0.963.83, allows remote attackers to cause a denial of service via vectors that trigger an invalid read operation.
CVE-2011-3058	Google Chrome before 18.0.1025.142 does not properly handle the EUC-JP encoding system, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.
CVE-2011-3059	Google Chrome before 18.0.1025.142 does not properly handle SVG text elements, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3060	Google Chrome before 18.0.1025.142 does not properly handle text fragments, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3061	Google Chrome before 18.0.1025.142 does not properly check X.509 certificates before use of a SPDY proxy, which might allow man-in-the-middle attackers to spoof servers or obtain sensitive information via a crafted certificate.
CVE-2011-3062	Off-by-one error in the OpenType Sanitizer in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted OpenType file.
CVE-2011-3063	Google Chrome before 18.0.1025.142 does not properly validate the renderer's navigation requests, which has unspecified impact and remote attack vectors.
CVE-2011-3064	Use-after-free vulnerability in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG clipping.
CVE-2011-3065	Skia, as used in Google Chrome before 18.0.1025.142, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3066	Skia, as used in Google Chrome before 18.0.1025.151, does not properly perform clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3067	Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to replacement of IFRAME elements.

CVE-2011-3068	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to run-in boxes.
CVE-2011-3069	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to line boxes.
CVE-2011-3070	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.
CVE-2011-3071	Use-after-free vulnerability in the HTMLMediaElement implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3072	Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to pop-up windows.
CVE-2011-3073	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG resources.
CVE-2011-3074	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media.
CVE-2011-3075	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style-application commands.
CVE-2011-3076	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to focus handling.
CVE-2011-3077	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the script bindings, related to a "read-after-free" issue.
CVE-2011-3078	Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3081.
CVE-2011-3080	Race condition in the Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168 allows attackers to bypass intended sandbox restrictions via unspecified vectors.
CVE-2011-3081	Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3078.
CVE-2011-3083	browser/profiles/profile_impl_io_data.cc in Google Chrome before 19.0.1084.46 does not properly handle a malformed ftp URL in the SRC attribute of a VIDEO element, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted web page.
CVE-2011-3084	Google Chrome before 19.0.1084.46 does not use a dedicated process for the loading of links found on an internal page, which might allow attackers to bypass intended sandbox restrictions via a crafted page.
CVE-2011-3085	The Autofill feature in Google Chrome before 19.0.1084.46 does not properly restrict field values, which allows remote attackers to cause a denial of service (UI corruption) and possibly conduct spoofing attacks via vectors involving long values.
CVE-2011-3086	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a STYLE element.
CVE-2011-3087	Google Chrome before 19.0.1084.46 does not properly perform window navigation, which has unspecified impact and remote attack vectors.
CVE-2011-3088	Google Chrome before 19.0.1084.46 does not properly draw hairlines, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3089	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving tables.
CVE-2011-3090	Race condition in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker processes.
CVE-2011-3091	Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3092	The regex implementation in Google V8, as used in Google Chrome before 19.0.1084.46, allows remote attackers to cause a denial of service (invalid write operation) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3093	Google Chrome before 19.0.1084.46 does not properly handle glyphs, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3094	Google Chrome before 19.0.1084.46 does not properly handle Tibetan text, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3095	The OGG container in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.

CVE-2011-3096	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an error in the GTK implementation of the omnibox.
CVE-2011-3097	The PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an out-of-bounds write error in the implementation of sampled functions.
CVE-2011-3098	Google Chrome before 19.0.1084.46 on Windows uses an incorrect search path for the Windows Media Player plug-in, which might allow local users to gain privileges via a Trojan horse plug-in in an unspecified directory.
CVE-2011-3099	Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a malformed name for the font encoding.
CVE-2011-3100	Google Chrome before 19.0.1084.46 does not properly draw dash paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3101	Google Chrome before 19.0.1084.46 on Linux does not properly mitigate an unspecified flaw in an NVIDIA driver, which has unknown impact and attack vectors. NOTE: see CVE-2012-3105 for the related MFSA 2012-34 issue in Mozilla products.
CVE-2011-3102	Off-by-one error in libxml2, as used in Google Chrome before 19.0.1084.46 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3103	Google V8, as used in Google Chrome before 19.0.1084.52, does not properly perform garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2011-3104	Skia, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3105	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2011-3106	The WebSockets implementation in Google Chrome before 19.0.1084.52 does not properly handle use of SSL, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3107	Google Chrome before 19.0.1084.52 does not properly implement JavaScript bindings for plug-ins, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3108	Use-after-free vulnerability in Google Chrome before 19.0.1084.52 allows remote attackers to execute arbitrary code via vectors related to the browser cache.
CVE-2011-3109	Google Chrome before 19.0.1084.52 on Linux does not properly perform a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact by leveraging an error in the GTK implementation of the UI.
CVE-2011-3110	The PDF functionality in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2011-3111	Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (invalid read operation) via unspecified vectors.
CVE-2011-3112	Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an invalid encrypted document.
CVE-2011-3113	The PDF functionality in Google Chrome before 19.0.1084.52 does not properly perform a cast of an unspecified variable during handling of color spaces, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3114	Multiple buffer overflows in the PDF functionality in Google Chrome before 19.0.1084.52 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unknown function calls.
CVE-2011-3115	Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger "type corruption."
CVE-2011-3234	Google Chrome before 14.0.835.163 does not properly handle boxes, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3389	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
CVE-2011-3640	** DISPUTED ** Untrusted search path vulnerability in Mozilla Network Security Services (NSS), as used in Google Chrome before 17 on Windows and Mac OS X, might allow local users to gain privileges via a Trojan

	horse pkcs11.txt file in a top-level directory. NOTE: the vendor's response was "Strange behavior, but we're not treating this as a security bug."
CVE-2011-3873	Google Chrome before 14.0.835.202 does not properly implement shader translation, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3875	Google Chrome before 15.0.874.102 does not properly handle drag and drop operations on URL strings, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3876	Google Chrome before 15.0.874.102 does not properly handle downloading files that have whitespace characters at the end of a filename, which has unspecified impact and user-assisted remote attack vectors.
CVE-2011-3877	Cross-site scripting (XSS) vulnerability in the appcache internals page in Google Chrome before 15.0.874.102 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-3878	Race condition in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker process initialization.
CVE-2011-3879	Google Chrome before 15.0.874.102 does not prevent redirects to chrome: URLs, which has unspecified impact and remote attack vectors.
CVE-2011-3880	Google Chrome before 15.0.874.102 does not prevent use of an unspecified special character as a delimiter in HTTP headers, which has unknown impact and remote attack vectors.
CVE-2011-3881	WebKit, as used in Google Chrome before 15.0.874.102 and Android before 4.4, allows remote attackers to bypass the Same Origin Policy and conduct Universal XSS (UXSS) attacks via vectors related to (1) the DOMWindow::clear function and use of a selection object, (2) the Object::GetRealNamedPropertyInPrototypeChain function and use of an __proto__ property, (3) the HTMLPlugInImageElement::allowedToLoadFrameURL function and use of a javascript: URL, (4) incorrect origins for XSLT-generated documents in the XSLTProcessor::createDocumentFromSource function, and (5) improper handling of synchronous frame loads in the ScriptController::executeIfJavaScriptURL function.
CVE-2011-3882	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media buffers.
CVE-2011-3883	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to counters.
CVE-2011-3884	Google Chrome before 15.0.874.102 does not properly address timing issues during DOM traversal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-3885	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to stale Cascading Style Sheets (CSS) token-sequence data.
CVE-2011-3886	Google V8, as used in Google Chrome before 15.0.874.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers out-of-bounds write operations.
CVE-2011-3887	Google Chrome before 15.0.874.102 does not properly handle javascript: URLs, which allows remote attackers to bypass intended access restrictions and read cookies via unspecified vectors.
CVE-2011-3888	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing operations in conjunction with an unknown plug-in.
CVE-2011-3889	Heap-based buffer overflow in the Web Audio implementation in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3890	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video source handling.
CVE-2011-3891	Google Chrome before 15.0.874.102 does not properly restrict access to internal Google V8 functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3892	Double free vulnerability in the Theora decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.
CVE-2011-3893	Google Chrome before 15.0.874.120 does not properly implement the MKV and Vorbis media handlers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3894	Google Chrome before 15.0.874.120 does not properly perform VP8 decoding, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted stream.
CVE-2011-3895	Heap-based buffer overflow in the Vorbis decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.
CVE-2011-3896	Buffer overflow in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to shader variable mapping.
CVE-2011-3897	Use-after-free vulnerability in Google Chrome before 15.0.874.120 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing.
CVE-2011-3898	Google Chrome before 15.0.874.120, when Java Runtime Environment (JRE) 7 is used, does not request user confirmation before applet execution begins, which allows remote attackers to have an unspecified impact via a crafted applet.

CVE-2011-3900	Google V8, as used in Google Chrome before 15.0.874.121, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write operation.
CVE-2011-3903	Google Chrome before 16.0.912.63 does not properly perform regex matching, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3904	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to bidirectional text (aka bidi) handling.
CVE-2011-3905	libxml2, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3906	The PDF parser in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3907	The view-source feature in Google Chrome before 16.0.912.63 allows remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3908	Google Chrome before 16.0.912.63 does not properly parse SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3909	The Cascading Style Sheets (CSS) implementation in Google Chrome before 16.0.912.63 on 64-bit platforms does not properly manage property arrays, which allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3910	Google Chrome before 16.0.912.63 does not properly handle YUV video frames, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3911	Google Chrome before 16.0.912.63 does not properly handle PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3912	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.
CVE-2011-3913	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to Range handling.
CVE-2011-3914	The internationalization (aka i18n) functionality in Google V8, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-3915	Buffer overflow in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF fonts.
CVE-2011-3916	Google Chrome before 16.0.912.63 does not properly handle PDF cross references, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3917	Stack-based buffer overflow in FileWatcher in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3919	Heap-based buffer overflow in libxml2, as used in Google Chrome before 16.0.912.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3921	Use-after-free vulnerability in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving animation frames.
CVE-2011-3922	Stack-based buffer overflow in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to glyph handling.
CVE-2011-3924	Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM selections.
CVE-2011-3925	Use-after-free vulnerability in the Safe Browsing feature in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors related to a navigation entry and an interstitial page.
CVE-2011-3926	Heap-based buffer overflow in the tree builder in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3927	Skia, as used in Google Chrome before 16.0.912.77, does not perform all required initialization of values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3928	Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM handling.
CVE-2011-3953	Google Chrome before 17.0.963.46 does not prevent monitoring of the clipboard after a paste event, which has unspecified impact and remote attack vectors.
CVE-2011-3954	Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via vectors that trigger a large amount of database usage.
CVE-2011-3955	Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that trigger the aborting of an IndexedDB transaction.
CVE-2011-3956	The extension implementation in Google Chrome before 17.0.963.46 does not properly handle sandboxed origins, which might allow remote attackers to bypass the Same Origin Policy via a crafted extension.

CVE-2011-3957	Use-after-free vulnerability in the garbage-collection functionality in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF documents.
CVE-2011-3958	Google Chrome before 17.0.963.46 does not properly perform casts of variables during handling of a column span, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-3959	Buffer overflow in the locale implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3960	Google Chrome before 17.0.963.46 does not properly decode audio data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3961	Race condition in Google Chrome before 17.0.963.46 allows remote attackers to execute arbitrary code via vectors that trigger a crash of a utility process.
CVE-2011-3962	Google Chrome before 17.0.963.46 does not properly perform path clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3963	Google Chrome before 17.0.963.46 does not properly handle PDF FAX images, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3964	Google Chrome before 17.0.963.46 does not properly implement the drag-and-drop feature, which makes it easier for remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3965	Google Chrome before 17.0.963.46 does not properly check signatures, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-3966	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to error handling for Cascading Style Sheets (CSS) token-sequence data.
CVE-2011-3967	Unspecified vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via a crafted certificate.
CVE-2011-3968	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving Cascading Style Sheets (CSS) token sequences.
CVE-2011-3969	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout of SVG documents.
CVE-2011-3970	libxslt, as used in Google Chrome before 17.0.963.46, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3971	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to mousemove events.
CVE-2011-3972	The shader translator implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-4691	Google Chrome 15.0.874.121 and earlier does not prevent capture of data about the times of Same Origin Policy violations during IFRAAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.
CVE-2011-4692	WebKit, as used in Apple Safari 5.1.1 and earlier and Google Chrome 15 and earlier, does not prevent capture of data about the time required for image loading, which makes it easier for remote attackers to determine whether an image exists in the browser cache via crafted JavaScript code, as demonstrated by visipisi.
CVE-2011-5319	content/renderer/device_sensors/device_motion_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate accelerometer data, which makes it easier for remote attackers to capture keystrokes via a crafted web site that listens for ondevicemotion events, a different vulnerability than CVE-2015-1231.
CVE-2012-0724	Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0725.
CVE-2012-0725	Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0724.
CVE-2012-1521	Use-after-free vulnerability in the XML parser in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-1845	Use-after-free vulnerability in Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the DEP and ASLR protection mechanisms, and execute arbitrary code, via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code."
CVE-2012-1846	Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the sandbox protection mechanism by leveraging access to a sandboxed process, as demonstrated by VUPEN during a Pwn2Own competition at

	CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code."
CVE-2012-2647	Yahoo! Toolbar 1.0.0.5 and earlier for Chrome and Safari allows remote attackers to modify the configured search URL, and intercept search terms, via a crafted web page.
CVE-2012-2764	Untrusted search path vulnerability in Google Chrome before 20.0.1132.43 on Windows might allow local users to gain privileges via a Trojan horse Metro DLL in the current working directory.
CVE-2012-2807	Multiple integer overflows in libxml2, as used in Google Chrome before 20.0.1132.43 and other products, on 64-bit Linux platforms allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2815	Google Chrome before 20.0.1132.43 allows remote attackers to obtain potentially sensitive information from a fragment identifier by leveraging access to an IFRAME element associated with a different domain.
CVE-2012-2816	Google Chrome before 20.0.1132.43 on Windows does not properly isolate sandboxed processes, which might allow remote attackers to cause a denial of service (process interference) via unspecified vectors.
CVE-2012-2817	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to tables that have sections.
CVE-2012-2818	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the layout of documents that use the Cascading Style Sheets (CSS) counters feature.
CVE-2012-2819	The texSubImage2D implementation in the WebGL subsystem in Google Chrome before 20.0.1132.43 does not properly handle uploads to floating-point textures, which allows remote attackers to cause a denial of service (assertion failure and application crash) or possibly have unspecified other impact via a crafted web page, as demonstrated by certain WebGL performance tests, aka rdar problem 11520387.
CVE-2012-2820	Google Chrome before 20.0.1132.43 does not properly implement SVG filters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2821	The autofill implementation in Google Chrome before 20.0.1132.43 does not properly display text, which has unspecified impact and remote attack vectors.
CVE-2012-2822	The PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2823	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG resources.
CVE-2012-2824	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG painting.
CVE-2012-2825	The XSL implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.
CVE-2012-2826	Google Chrome before 20.0.1132.43 does not properly implement texture conversion, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2827	Use-after-free vulnerability in the UI in Google Chrome before 20.0.1132.43 on Mac OS X allows attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2828	Multiple integer overflows in the PDF functionality in Google Chrome before 20.0.1132.43 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2829	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2012-2830	Google Chrome before 20.0.1132.43 does not properly set array values, which allows remote attackers to cause a denial of service (incorrect pointer use) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2831	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG references.
CVE-2012-2832	The image-codec implementation in the PDF functionality in Google Chrome before 20.0.1132.43 does not initialize an unspecified pointer, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2012-2833	Buffer overflow in the JS API in the PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2834	Integer overflow in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted data in the Matroska container format.
CVE-2012-2842	Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to counter handling.
CVE-2012-2843	Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout height tracking.
CVE-2012-2844	The PDF functionality in Google Chrome before 20.0.1132.57 does not properly handle JavaScript code, which allows remote attackers to cause a denial of service (incorrect object access) or possibly have unspecified other impact via a crafted document.

CVE-2012-2846	Google Chrome before 21.0.1180.57 on Linux does not properly isolate renderer processes, which allows remote attackers to cause a denial of service (cross-process interference) via unspecified vectors.
CVE-2012-2847	Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not request user confirmation before continuing a large series of downloads, which allows user-assisted remote attackers to cause a denial of service (resource consumption) via a crafted web site.
CVE-2012-2848	The drag-and-drop implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to bypass intended file access restrictions via a crafted web site.
CVE-2012-2849	Off-by-one error in the GIF decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image.
CVE-2012-2850	Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to have an unknown impact via a crafted document.
CVE-2012-2851	Multiple integer overflows in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2852	The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly handle object linkage, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted document.
CVE-2012-2853	The webRequest API in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly interact with the Chrome Web Store, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.
CVE-2012-2854	Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to obtain potentially sensitive information about pointer values by leveraging access to a WebUI renderer process.
CVE-2012-2855	Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2856	The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2857	Use-after-free vulnerability in the Cascading Style Sheets (CSS) DOM implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2858	Buffer overflow in the WebP decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted WebP image.
CVE-2012-2859	Google Chrome before 21.0.1180.57 on Linux does not properly handle tabs, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2860	The date-picker implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.
CVE-2012-2862	Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2863	The PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2865	Google Chrome before 21.0.1180.89 does not properly perform line breaking, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2012-2866	Google Chrome before 21.0.1180.89 does not properly perform a cast of an unspecified variable during handling of run-in elements, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2012-2867	The SPDY implementation in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2868	Race condition in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving improper interaction between worker processes and an XMLHttpRequest (aka XHR) object.
CVE-2012-2869	Google Chrome before 21.0.1180.89 does not properly load URLs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a "stale buffer."
CVE-2012-2870	libxslt 1.1.26 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly manage memory, which might allow remote attackers to cause a denial of service (application crash) via a crafted XSLT expression

	that is not properly identified during XPath navigation, related to (1) the <code>xsltCompileLocationPathPattern</code> function in <code>libxslt/pattern.c</code> and (2) the <code>xsltGenerateIdFunction</code> function in <code>libxslt/functions.c</code> .
CVE-2012-2871	libxml2 2.9.0-rc1 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly support a cast of an unspecified variable during handling of XSL transforms, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document, related to the <code>_xmlNs</code> data structure in <code>include/libxml/tree.h</code> .
CVE-2012-2872	Cross-site scripting (XSS) vulnerability in an SSL interstitial page in Google Chrome before 21.0.1180.89 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-2874	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2883.
CVE-2012-2875	Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 22.0.1229.79 allow remote attackers to have an unknown impact via a crafted document.
CVE-2012-2876	Buffer overflow in the SSE2 optimization functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2877	The extension system in Google Chrome before 22.0.1229.79 does not properly handle modal dialogs, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2878	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.
CVE-2012-2879	Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service (DOM topology corruption) via a crafted document.
CVE-2012-2880	Race condition in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the plug-in paint buffer.
CVE-2012-2881	Google Chrome before 22.0.1229.79 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2882	FFmpeg, as used in Google Chrome before 22.0.1229.79, does not properly handle OGG containers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "wild pointer" issue.
CVE-2012-2883	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2874.
CVE-2012-2884	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2885	Double free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to application exit.
CVE-2012-2886	Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors related to the Google V8 bindings, aka "Universal XSS (UXSS)."
CVE-2012-2887	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving onclick events.
CVE-2012-2888	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG text references.
CVE-2012-2889	Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors involving frames, aka "Universal XSS (UXSS)."
CVE-2012-2890	Use-after-free vulnerability in the PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2891	The IPC implementation in Google Chrome before 22.0.1229.79 allows attackers to obtain potentially sensitive information about memory addresses via unspecified vectors.
CVE-2012-2892	Unspecified vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2012-2893	Double free vulnerability in libxslt, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XSL transforms.
CVE-2012-2894	Google Chrome before 22.0.1229.79 does not properly handle graphics-context data structures, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2895	The PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2896	Integer overflow in the WebGL implementation in Google Chrome before 22.0.1229.79 on Mac OS X allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2897	The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT, as used by Google Chrome before 22.0.1229.79 and other programs, do not properly handle objects

	in memory, which allows remote attackers to execute arbitrary code via a crafted TrueType font file, aka "Windows Font Parsing Vulnerability" or "TrueType Font Parsing Vulnerability."
CVE-2012-2898	Google Chrome before 21.0.1180.82 on iOS on iPad devices allows remote attackers to spoof the Omnibox URL via vectors involving SSL error messages, a related issue to CVE-2012-0674.
CVE-2012-2899	Google Chrome before 21.0.1180.82 on iOS makes certain incorrect calls to WebView methods that trigger use of an applewebdata: URL, which allows remote attackers to bypass the Same Origin Policy and conduct Universal XSS (UXSS) attacks via vectors involving the document.write method.
CVE-2012-2900	Skia, as used in Google Chrome before 22.0.1229.92, does not properly render text, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2012-4903	Google Chrome before 18.0.1025308 on Android does not properly restrict access to file: URLs, which allows remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by obtaining credential data, a different vulnerability than CVE-2012-4906.
CVE-2012-4904	Cross-application scripting vulnerability in Google Chrome before 18.0.1025308 on Android allows remote attackers to inject arbitrary web script via unspecified vectors, as demonstrated by "Universal XSS (UXSS)" attacks against the current tab.
CVE-2012-4905	Cross-site scripting (XSS) vulnerability in Google Chrome before 18.0.1025308 on Android allows remote attackers to inject arbitrary web script or HTML via an extra in an Intent object, aka "Universal XSS (UXSS)."
CVE-2012-4906	Google Chrome before 18.0.1025308 on Android does not properly restrict access to file: URLs, which allows remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by obtaining credential data, a different vulnerability than CVE-2012-4903.
CVE-2012-4907	Google Chrome before 18.0.1025308 on Android does not properly restrict access from JavaScript code to Android APIs, which allows remote attackers to have an unspecified impact via a crafted web page.
CVE-2012-4908	Google Chrome before 18.0.1025308 on Android allows remote attackers to bypass the Same Origin Policy and obtain access to local files via vectors involving a symlink.
CVE-2012-4909	Google Chrome before 18.0.1025308 on Android allows remote attackers to obtain cookie information via a crafted application.
CVE-2012-4929	The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.
CVE-2012-4930	The SPDY protocol 3 and earlier, as used in Mozilla Firefox, Google Chrome, and other products, can perform TLS encryption of compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.
CVE-2012-5108	Race condition in Google Chrome before 22.0.1229.92 allows remote attackers to execute arbitrary code via vectors related to audio devices.
CVE-2012-5109	The International Components for Unicode (ICU) functionality in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a regular expression.
CVE-2012-5110	The compositor in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5111	Google Chrome before 22.0.1229.92 does not monitor for crashes of Pepper plug-ins, which has unspecified impact and remote attack vectors.
CVE-2012-5112	Use-after-free vulnerability in the SVG implementation in WebKit, as used in Google Chrome before 22.0.1229.94, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5115	Google Chrome before 23.0.1271.64 on Mac OS X does not properly mitigate improper write behavior in graphics drivers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger "wild writes."
CVE-2012-5116	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG filters.
CVE-2012-5117	Google Chrome before 23.0.1271.64 does not properly restrict the loading of an SVG subresource in the context of an IMG element, which has unspecified impact and remote attack vectors.
CVE-2012-5118	Google Chrome before 23.0.1271.64 on Mac OS X does not properly validate an integer value during the handling of GPU command buffers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5119	Race condition in Pepper, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to buffers.
CVE-2012-5120	Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, on 64-bit Linux platforms allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to an array.

CVE-2012-5121	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video layout.
CVE-2012-5122	Google Chrome before 23.0.1271.64 does not properly perform a cast of an unspecified variable during handling of input, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2012-5123	Skia, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5124	Google Chrome before 23.0.1271.64 does not properly handle textures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2012-5125	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.
CVE-2012-5126	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of plug-in placeholders.
CVE-2012-5127	Integer overflow in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted WebP image.
CVE-2012-5128	Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, does not properly perform write operations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5129	Heap-based buffer overflow in the WebGL subsystem in Google Chrome OS before 23.0.1271.94 allows remote attackers to cause a denial of service (GPU process crash) or possibly have unspecified other impact via unknown vectors.
CVE-2012-5130	Skia, as used in Google Chrome before 23.0.1271.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5131	Google Chrome before 23.0.1271.91 on Mac OS X does not properly mitigate improper rendering behavior in the Intel GPU driver, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5132	Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service (application crash) via a response with chunked transfer coding.
CVE-2012-5133	Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.
CVE-2012-5134	Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c in libxml2 2.9.0 and earlier, as used in Google Chrome before 23.0.1271.91 and other products, allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted entities in an XML document.
CVE-2012-5135	Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.
CVE-2012-5136	Google Chrome before 23.0.1271.91 does not properly perform a cast of an unspecified variable during handling of the INPUT element, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document.
CVE-2012-5137	Use-after-free vulnerability in Google Chrome before 23.0.1271.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Media Source API.
CVE-2012-5138	Google Chrome before 23.0.1271.95 does not properly handle file paths, which has unspecified impact and attack vectors.
CVE-2012-5139	Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to visibility events.
CVE-2012-5140	Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the URL loader.
CVE-2012-5141	Google Chrome before 23.0.1271.97 does not properly restrict instantiation of the Chromoting client plug-in, which has unspecified impact and attack vectors.
CVE-2012-5142	Google Chrome before 23.0.1271.97 does not properly handle history navigation, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.
CVE-2012-5143	Integer overflow in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PPAPI image buffers.
CVE-2012-5144	Google Chrome before 23.0.1271.97, and Libav 0.7.x before 0.7.7 and 0.8.x before 0.8.5, do not properly perform AAC decoding, which allows remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via vectors related to "an off-by-one overwrite when switching to LTP profile from MAIN."
CVE-2012-5145	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG layout.
CVE-2012-5146	Google Chrome before 24.0.1312.52 allows remote attackers to bypass the Same Origin Policy via a malformed URL.

CVE-2012-5147	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM handling.
CVE-2012-5148	The hyphenation functionality in Google Chrome before 24.0.1312.52 does not properly validate file names, which has unspecified impact and attack vectors.
CVE-2012-5149	Integer overflow in the audio IPC layer in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5150	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving seek operations on video data.
CVE-2012-5151	Integer overflow in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code in a PDF document.
CVE-2012-5152	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving seek operations on video data.
CVE-2012-5153	Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to stack memory.
CVE-2012-5154	Integer overflow in Google Chrome before 24.0.1312.52 on Windows allows attackers to cause a denial of service or possibly have unspecified other impact via vectors related to allocation of shared memory.
CVE-2012-5155	Google Chrome before 24.0.1312.52 on Mac OS X does not use an appropriate sandboxing approach for worker processes, which makes it easier for remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2012-5156	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF fields.
CVE-2012-5157	Google Chrome before 24.0.1312.52 does not properly handle image data in PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2012-5376	The Inter-process Communication (IPC) implementation in Google Chrome before 22.0.1229.94 allows remote attackers to bypass intended sandbox restrictions and write to arbitrary files by leveraging access to a renderer process, a different vulnerability than CVE-2012-5112.
CVE-2012-5851	html/parser/XSSAuditor.cpp in WebCore in WebKit, as used in Google Chrome through 22 and Safari 5.1.7, does not consider all possible output contexts of reflected data, which makes it easier for remote attackers to bypass a cross-site scripting (XSS) protection mechanism via a crafted string, aka rdar problem 12019108.
CVE-2013-0828	The PDF functionality in Google Chrome before 24.0.1312.52 does not properly perform a cast of an unspecified variable during processing of the root of the structure tree, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2013-0829	Google Chrome before 24.0.1312.52 does not properly maintain database metadata, which allows remote attackers to bypass intended file-access restrictions via unspecified vectors.
CVE-2013-0830	The IPC layer in Google Chrome before 24.0.1312.52 on Windows omits a NUL character required for termination of an unspecified data structure, which has unknown impact and attack vectors.
CVE-2013-0831	Directory traversal vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to have an unspecified impact by leveraging access to an extension process.
CVE-2013-0832	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.
CVE-2013-0833	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to printing.
CVE-2013-0834	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving glyphs.
CVE-2013-0835	Unspecified vulnerability in the Geolocation implementation in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2013-0836	Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, does not properly implement garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2013-0837	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.
CVE-2013-0838	Google Chrome before 24.0.1312.52 on Linux uses weak permissions for shared memory segments, which has unspecified impact and attack vectors.
CVE-2013-0839	Use-after-free vulnerability in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of fonts in CANVAS elements.
CVE-2013-0840	Google Chrome before 24.0.1312.56 does not validate URLs during the opening of new windows, which has unspecified impact and remote attack vectors.
CVE-2013-0841	Array index error in the content-blocking functionality in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0842	Google Chrome before 24.0.1312.56 does not properly handle %00 characters in pathnames, which has unspecified impact and attack vectors.

CVE-2013-0843	content/renderer/media/webrtc_audio_renderer.cc in Google Chrome before 24.0.1312.56 on Mac OS X does not use an appropriate buffer size for the 96 kHz sampling rate, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a web site that provides WebRTC audio.
CVE-2013-0879	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly implement web audio nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0880	Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to databases.
CVE-2013-0881	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via crafted data in the Matroska container format.
CVE-2013-0882	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via a large number of SVG parameters.
CVE-2013-0883	Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.
CVE-2013-0884	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly load Native Client (aka NaCl) code, which has unspecified impact and attack vectors.
CVE-2013-0885	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict API privileges during interaction with the Chrome Web Store, which has unspecified impact and attack vectors.
CVE-2013-0886	Google Chrome before 25.0.1364.99 on Mac OS X does not properly implement signal handling for Native Client (aka NaCl) code, which has unspecified impact and attack vectors.
CVE-2013-0887	The developer-tools process in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict privileges during interaction with a connected server, which has unspecified impact and attack vectors.
CVE-2013-0888	Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a "user gesture check for dangerous file downloads."
CVE-2013-0889	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly enforce a user gesture requirement before proceeding with a file download, which might make it easier for remote attackers to execute arbitrary code via a crafted file.
CVE-2013-0890	Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service (memory corruption) or possibly have other impact via unknown vectors.
CVE-2013-0891	Integer overflow in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a blob.
CVE-2013-0892	Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-0893	Race condition in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media.
CVE-2013-0894	Buffer overflow in the vorbis_parse_setup_hdr_floors function in the Vorbis decoder in vorbisdec.c in libavcodec in FFmpeg through 1.1.3, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (divide-by-zero error or out-of-bounds array access) or possibly have unspecified other impact via vectors involving a zero value for a bark map size.
CVE-2013-0895	Google Chrome before 25.0.1364.97 on Linux, and before 25.0.1364.99 on Mac OS X, does not properly handle pathnames during copy operations, which might make it easier for remote attackers to execute arbitrary programs via unspecified vectors.
CVE-2013-0896	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly manage memory during message handling for plug-ins, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0897	Off-by-one error in the PDF functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service via a crafted document.
CVE-2013-0898	Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a URL.

CVE-2013-0899	Integer overflow in the padding implementation in the opus_packet_parse_impl function in src/opus_decoder.c in Opus before 1.0.2, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a long packet.
CVE-2013-0900	Race condition in the International Components for Unicode (ICU) functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0902	Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0903	Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of browser navigation.
CVE-2013-0904	The Web Audio implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0905	Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG animation.
CVE-2013-0906	The IndexedDB implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0907	Race condition in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media threads.
CVE-2013-0908	Google Chrome before 25.0.1364.152 does not properly manage bindings of extension processes, which has unspecified impact and attack vectors.
CVE-2013-0909	The XSS Auditor in Google Chrome before 25.0.1364.152 allows remote attackers to obtain sensitive HTTP Referer information via unspecified vectors.
CVE-2013-0910	Google Chrome before 25.0.1364.152 does not properly manage the interaction between the browser process and renderer processes during authorization of the loading of a plug-in, which makes it easier for remote attackers to bypass intended access restrictions via vectors involving a blocked plug-in.
CVE-2013-0911	Directory traversal vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to have an unspecified impact via vectors related to databases.
CVE-2013-0912	WebKit in Google Chrome before 25.0.1364.160 allows remote attackers to execute arbitrary code via vectors that leverage "type confusion."
CVE-2013-0916	Use-after-free vulnerability in the Web Audio implementation in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0917	The URL loader in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-0918	Google Chrome before 26.0.1410.43 does not prevent navigation to developer tools in response to a drag-and-drop operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-0919	Use-after-free vulnerability in Google Chrome before 26.0.1410.43 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the presence of an extension that creates a pop-up window.
CVE-2013-0920	Use-after-free vulnerability in the extension bookmarks API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0921	The Isolated Sites feature in Google Chrome before 26.0.1410.43 does not properly enforce the use of separate processes, which makes it easier for remote attackers to bypass intended access restrictions via a crafted web site.
CVE-2013-0922	Google Chrome before 26.0.1410.43 does not properly restrict brute-force access attempts against web sites that require HTTP Basic Authentication, which has unspecified impact and attack vectors.
CVE-2013-0923	The USB Apps API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-0924	The extension functionality in Google Chrome before 26.0.1410.43 does not verify that use of the permissions API is consistent with file permissions, which has unspecified impact and attack vectors.
CVE-2013-0925	Google Chrome before 26.0.1410.43 does not ensure that an extension has the tabs (aka APIPermission:kTab) permission before providing a URL to this extension, which has unspecified impact and remote attack vectors.
CVE-2013-0926	Google Chrome before 26.0.1410.43 does not properly handle active content in an EMBED element during a copy-and-paste operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-1489	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 10 and Update 11, when running on Windows using Internet Explorer, Firefox, Opera, and Google Chrome, allows remote attackers to bypass the "Very High" security level of the Java Control Panel and execute unsigned Java code without prompting the user via unknown vectors, aka "Issue 53" and the "Java Security Slider" vulnerability.
CVE-2013-2268	Unspecified vulnerability in the MathML implementation in WebKit in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, has unknown impact and remote attack vectors, related to a "high severity security issue."

CVE-2013-2566	The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.
CVE-2013-2632	Google V8 before 3.17.13, as used in Google Chrome before 27.0.1444.3, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by the Bejeweled game.
CVE-2013-2836	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.93 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2837	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2838	Google V8, as used in Google Chrome before 27.0.1453.93, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2839	Google Chrome before 27.0.1453.93 does not properly perform a cast of an unspecified variable during handling of clipboard data, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2840	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2846.
CVE-2013-2841	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of Pepper resources.
CVE-2013-2842	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of widgets.
CVE-2013-2843	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of speech data.
CVE-2013-2844	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style resolution.
CVE-2013-2845	The Web Audio implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2846	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2840.
CVE-2013-2847	Race condition in the workers implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2848	The XSS Auditor in Google Chrome before 27.0.1453.93 might allow remote attackers to obtain sensitive information via unspecified vectors.
CVE-2013-2849	Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome before 27.0.1453.93 allow user-assisted remote attackers to inject arbitrary web script or HTML via vectors involving a (1) drag-and-drop or (2) copy-and-paste operation.
CVE-2013-2853	The HTTPS implementation in Google Chrome before 28.0.1500.71 does not ensure that headers are terminated by <code>\r\n\r\n</code> (carriage return, newline, carriage return, newline), which allows man-in-the-middle attackers to have an unspecified impact via vectors that trigger header truncation.
CVE-2013-2854	Google Chrome before 27.0.1453.110 on Windows provides an incorrect handle to a renderer process in unspecified circumstances, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2855	The Developer Tools API in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2856	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2857	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of images.
CVE-2013-2858	Use-after-free vulnerability in the HTML5 Audio implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2859	Google Chrome before 27.0.1453.110 allows remote attackers to bypass the Same Origin Policy and trigger namespace pollution via unspecified vectors.
CVE-2013-2860	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving access to a database API by a worker process.
CVE-2013-2861	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

CVE-2013-2862	Skia, as used in Google Chrome before 27.0.1453.110, does not properly handle GPU acceleration, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2863	Google Chrome before 27.0.1453.110 does not properly handle SSL sockets, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-2864	The PDF functionality in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2865	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.110 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2866	The Flash plug-in in Google Chrome before 27.0.1453.116, as used on Google Chrome OS before 27.0.1453.116 and separately, does not properly determine whether a user wishes to permit camera or microphone access by a Flash application, which allows remote attackers to obtain sensitive information from a machine's physical environment via a clickjacking attack, as demonstrated by an attack using a crafted Cascading Style Sheets (CSS) opacity property.
CVE-2013-2867	Google Chrome before 28.0.1500.71 does not properly prevent pop-under windows, which allows remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-2868	common/extensions/sync_helper.cc in Google Chrome before 28.0.1500.71 proceeds with sync operations for NPAPI extensions without checking for a certain plugin permission setting, which might allow remote attackers to trigger unwanted extension changes via unspecified vectors.
CVE-2013-2869	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted JPEG2000 image.
CVE-2013-2870	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote servers to execute arbitrary code via crafted response traffic after a URL request.
CVE-2013-2871	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2872	Google Chrome before 28.0.1500.71 on Mac OS X does not ensure a sufficient source of entropy for renderer processes, which might make it easier for remote attackers to defeat cryptographic protection mechanisms in third-party components via unspecified vectors.
CVE-2013-2873	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a 404 HTTP status code during the loading of resources.
CVE-2013-2874	Google Chrome before 28.0.1500.71 on Windows, when an Nvidia GPU is used, allows remote attackers to bypass intended restrictions on access to screen data via vectors involving IPC transmission of GL textures.
CVE-2013-2875	core/rendering/svg/SVGInlineTextBox.cpp in the SVG implementation in Blink, as used in Google Chrome before 28.0.1500.71, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2876	browser/extensions/api/tabs/tabs_api.cc in Google Chrome before 28.0.1500.71 does not properly enforce restrictions on the capture of screenshots by extensions, which allows remote attackers to obtain sensitive information about the content of a previous page via vectors involving an interstitial page.
CVE-2013-2877	parser.c in libxml2 before 2.9.0, as used in Google Chrome before 28.0.1500.71 and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a document that ends abruptly, related to the lack of certain checks for the XML_PARSER_EOF state.
CVE-2013-2878	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the handling of text.
CVE-2013-2879	Google Chrome before 28.0.1500.71 does not properly determine the circumstances in which a renderer process can be considered a trusted process for sign-in and subsequent sync operations, which makes it easier for remote attackers to conduct phishing attacks via a crafted web site.
CVE-2013-2880	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2881	Google Chrome before 28.0.1500.95 does not properly handle frames, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2013-2882	Google V8, as used in Google Chrome before 28.0.1500.95, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2013-2883	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to deleting the registration of a MutationObserver object.
CVE-2013-2884	Use-after-free vulnerability in the DOM implementation in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper tracking of which document owns an Attr object.
CVE-2013-2885	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to not properly considering focus during the processing of JavaScript events in the presence of a multiple-fields input type.

CVE-2013-2886	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.95 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2887	Multiple unspecified vulnerabilities in Google Chrome before 29.0.1547.57 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2900	The FilePath::ReferencesParent function in files/file_path.cc in Google Chrome before 29.0.1547.57 on Windows does not properly handle pathname components composed entirely of . (dot) and whitespace characters, which allows remote attackers to conduct directory traversal attacks via a crafted directory name.
CVE-2013-2901	Multiple integer overflows in (1) libGLESv2/renderer/Renderer9.cpp and (2) libGLESv2/renderer/Renderer11.cpp in Almost Native Graphics Layer Engine (ANGLE), as used in Google Chrome before 29.0.1547.57, allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2902	Use-after-free vulnerability in the XSLT ProcessingInstruction implementation in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to an applyXSLTransform call involving (1) an HTML document or (2) an xsl:processing-instruction element that is still in the process of loading.
CVE-2013-2903	Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving moving a (1) AUDIO or (2) VIDEO element between documents.
CVE-2013-2904	Use-after-free vulnerability in the Document::finishedParsing function in core/dom/Document.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via an onload event that changes an IFRAAME element so that its src attribute is no longer an XML document, leading to unintended garbage collection of this document.
CVE-2013-2905	The SharedMemory::Create function in memory/shared_memory_posix.cc in Google Chrome before 29.0.1547.57 uses weak permissions under /dev/shm/, which allows attackers to obtain sensitive information via direct access to a POSIX shared-memory file.
CVE-2013-2906	Multiple race conditions in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to threading in core/html/HTMLMediaElement.cpp, core/platform/audio/AudioDSPKernelProcessor.cpp, core/platform/audio/HRTFElevation.cpp, and modules/webaudio/ConvolverNode.cpp.
CVE-2013-2907	The Window.prototype object implementation in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2908	Google Chrome before 30.0.1599.66 uses incorrect function calls to determine the values of NavigationEntry objects, which allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code.
CVE-2013-2909	Use-after-free vulnerability in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to inline-block rendering for bidirectional Unicode text in an element isolated from its siblings.
CVE-2013-2910	Use-after-free vulnerability in modules/webaudio/AudioScheduledSourceNode.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2911	Use-after-free vulnerability in the XSLStyleSheet::compileStyleSheet function in core/xml/XSLStyleSheetLibxslt.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of post-failure recompilation in unspecified libxslt versions.
CVE-2013-2912	Use-after-free vulnerability in the PepperInProcessRouter::SendToHost function in content/renderer/pepper/pepper_in_process_router.cc in the Pepper Plug-in API (PPAPI) in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a resource-destruction message.
CVE-2013-2913	Use-after-free vulnerability in the XMLDocumentParser::append function in core/xml/parser/XMLDocumentParser.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an XML document.
CVE-2013-2914	Use-after-free vulnerability in the color-chooser dialog in Google Chrome before 30.0.1599.66 on Windows allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to color_chooser_dialog.cc and color_chooser_win.cc in browser/ui/views/.
CVE-2013-2915	Google Chrome before 30.0.1599.66 preserves pending NavigationEntry objects in certain invalid circumstances, which allows remote attackers to spoof the address bar via a URL with a malformed scheme, as demonstrated by a nonexistent:12121 URL.

CVE-2013-2916	Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code, in conjunction with a delay in notifying the user of an attempted spoof.
CVE-2013-2917	The ReverbConvolverStage::ReverbConvolverStage function in core/platform/audio/ReverbConvolverStage.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the impulseResponse array.
CVE-2013-2918	Use-after-free vulnerability in the RenderBlock::collapseAnonymousBlockChild function in core/rendering/RenderBlock.cpp in the DOM implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect handling of parent-child relationships for anonymous blocks.
CVE-2013-2919	Google V8, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2920	The DoResolveRelativeHost function in url/url_canon_relative.cc in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via a relative URL containing a hostname, as demonstrated by a protocol-relative URL beginning with a //www.google.com/ substring.
CVE-2013-2921	Double free vulnerability in the ResourceFetcher::didLoadResource function in core/fetch/ResourceFetcher.cpp in the resource loader in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering certain callback processing during the reporting of a resource entry.
CVE-2013-2922	Use-after-free vulnerability in core/html/HTMLTemplateElement.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that operates on a TEMPLATE element.
CVE-2013-2923	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.66 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2924	Use-after-free vulnerability in International Components for Unicode (ICU), as used in Google Chrome before 30.0.1599.66 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2925	Use-after-free vulnerability in core/xml/XMLHttpRequest.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger multiple conflicting uses of the same XMLHttpRequest object.
CVE-2013-2926	Use-after-free vulnerability in the IndentOutdentCommand::tryIndentingAsListItem function in core/editing/IndentOutdentCommand.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to list elements.
CVE-2013-2927	Use-after-free vulnerability in the HTMLFormElement::prepareForSubmission function in core/html/HTMLFormElement.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to submission for FORM elements.
CVE-2013-2928	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2931	Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.48 allow attackers to execute arbitrary code or possibly have other impact via unknown vectors.
CVE-2013-6166	Google Chrome before 29 sends HTTP Cookie headers without first validating that they have the required character-set restrictions, which allows remote attackers to conduct the equivalent of a persistent Logout CSRF attack via a crafted parameter that forces a web application to set a malformed cookie within an HTTP response.
CVE-2013-6621	Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the x-webkit-speech attribute in a text INPUT element.
CVE-2013-6622	Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the movement of a media element between documents.
CVE-2013-6623	The SVG implementation in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging the use of tree order, rather than transitive dependency order, for layout.
CVE-2013-6624	Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the string values of id attributes.
CVE-2013-6625	Use-after-free vulnerability in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of DOM range objects in circumstances that require child node removal after a (1) mutation or (2) blur event.

CVE-2013-6626	The WebContentsImpl::AttachInterstitialPage function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 31.0.1650.48 does not cancel JavaScript dialogs upon generating an interstitial warning, which allows remote attackers to spoof the address bar via a crafted web site.
CVE-2013-6627	net/http/http_stream_parser.cc in Google Chrome before 31.0.1650.48 does not properly process HTTP Informational (aka 1xx) status codes, which allows remote web servers to cause a denial of service (out-of-bounds read) via a crafted response.
CVE-2013-6628	net/socket/ssl_client_socket_nss.cc in the TLS implementation in Google Chrome before 31.0.1650.48 does not ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which might allow remote web servers to interfere with trust relationships by renegotiating a session.
CVE-2013-6629	The get_sos function in jdmarker.c in (1) libjpeg 6b and (2) libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48, Ghostscript, and other products, does not check for certain duplications of component data during the reading of segments that follow Start Of Scan (SOS) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.
CVE-2013-6630	The get_dht function in jdmarker.c in libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48 and other products, does not set all elements of a certain Huffman value array during the reading of segments that follow Define Huffman Table (DHT) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.
CVE-2013-6631	Use-after-free vulnerability in the Channel::SendRTCPPacket function in voice_engine/channel.cc in libjingle in WebRTC, as used in Google Chrome before 31.0.1650.48 and other products, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger the absence of certain statistics initialization, leading to the skipping of a required DeRegisterExternalTransport call.
CVE-2013-6632	Integer overflow in Google Chrome before 31.0.1650.57 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013.
CVE-2013-6634	The OneClickSigninHelper::ShowInfoBarIfPossible function in browser/ui/sync/one_click_signin_helper.cc in Google Chrome before 31.0.1650.63 uses an incorrect URL during realm validation, which allows remote attackers to conduct session fixation attacks and hijack web sessions by triggering improper sync after a 302 (aka Found) HTTP status code.
CVE-2013-6635	Use-after-free vulnerability in the editing implementation in Blink, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that triggers removal of a node during processing of the DOM tree, related to CompositeEditCommand.cpp and ReplaceSelectionCommand.cpp.
CVE-2013-6636	The FrameLoader::notifyIfInitialDocumentAccessed function in core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 31.0.1650.63, makes an incorrect check for an empty document during presentation of a modal dialog, which allows remote attackers to spoof the address bar via vectors involving the document.write method.
CVE-2013-6637	Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.63 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6638	Multiple buffer overflows in runtime.cc in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a large typed array, related to the (1) Runtime_TypedArrayInitialize and (2) Runtime_TypedArrayInitializeFromArrayLike functions.
CVE-2013-6639	The DehoistArrayIndex function in hydrogen-dehoist.cc (aka hydrogen.cc) in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via JavaScript code that sets the value of an array element with a crafted index.
CVE-2013-6640	The DehoistArrayIndex function in hydrogen-dehoist.cc (aka hydrogen.cc) in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service (out-of-bounds read) via JavaScript code that sets a variable to the value of an array element with a crafted index.
CVE-2013-6641	Use-after-free vulnerability in the FormAssociatedElement::formRemovedFromTree function in core/html/FormAssociatedElement.cpp in Blink, as used in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of the past names map of a FORM element.
CVE-2013-6642	Google Chrome through 32.0.1700.23 on Android allows remote attackers to spoof the address bar via unspecified vectors.
CVE-2013-6643	The OneClickSigninBubbleView::WindowClosing function in browser/ui/views/sync/one_click_signin_bubble_view.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog.

CVE-2013-6644	Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6645	Use-after-free vulnerability in the OnWindowRemovingFromRootWindow function in content/browser/web_contents/web_contents_view_aura.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving certain print-preview and tab-switch actions that interact with a speech input element.
CVE-2013-6646	Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the shutting down of a worker process.
CVE-2013-6649	Use-after-free vulnerability in the RenderSVGImage::paint function in core/rendering/svg/RenderSVGImage.cpp in Blink, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a zero-size SVG image.
CVE-2013-6650	The StoreBuffer::ExemptPopularPages function in store-buffer.cc in Google V8 before 3.22.24.16, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors that trigger incorrect handling of "popular pages."
CVE-2013-6652	Directory traversal vulnerability in sandbox/win/src/named_pipe_dispatcher.cc in Google Chrome before 33.0.1750.117 on Windows allows attackers to bypass intended named-pipe policy restrictions in the sandbox via vectors related to (1) lack of checks for .. (dot dot) sequences or (2) lack of use of the \\?\\ protection mechanism.
CVE-2013-6653	Use-after-free vulnerability in the web contents implementation in Google Chrome before 33.0.1750.117 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attempted conflicting access to the color chooser.
CVE-2013-6654	The SVGAnimateElement::calculateAnimatedValue function in core/svg/SVGAnimateElement.cpp in Blink, as used in Google Chrome before 33.0.1750.117, does not properly handle unexpected data types, which allows remote attackers to cause a denial of service (incorrect cast) or possibly have unspecified other impact via unknown vectors.
CVE-2013-6655	Use-after-free vulnerability in Blink, as used in Google Chrome before 33.0.1750.117, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper handling of overflowchanged DOM events during interaction between JavaScript and layout.
CVE-2013-6656	The XSSAuditor::init function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, processes POST requests by using the body of a redirecting page instead of the body of a redirect target, which allows remote attackers to obtain sensitive information via unspecified vectors.
CVE-2013-6657	core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, inserts the about:blank URL during certain blocking of FORM elements within HTTP requests, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2013-6658	Multiple use-after-free vulnerabilities in the layout implementation in Blink, as used in Google Chrome before 33.0.1750.117, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving (1) running JavaScript code during execution of the updateWidgetPositions function or (2) making a call into a plugin during execution of the updateWidgetPositions function.
CVE-2013-6659	The SSLClientSocketNSS::Core::OwnAuthCertHandler function in net/socket/ssl_client_socket_nss.cc in Google Chrome before 33.0.1750.117 does not prevent changes to server X.509 certificates during renegotiations, which allows remote SSL servers to trigger use of a new certificate chain, inconsistent with the user's expectations, by initiating a TLS renegotiation.
CVE-2013-6660	The drag-and-drop implementation in Google Chrome before 33.0.1750.117 does not properly restrict the information in WebDropData data structures, which allows remote attackers to discover full pathnames via a crafted web site.
CVE-2013-6661	Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.117 allow attackers to bypass the sandbox protection mechanism after obtaining renderer access, or have other impact, via unknown vectors.
CVE-2013-6663	Use-after-free vulnerability in the SVGImage::setContainerSize function in core/svg/graphics/SVGImage.cpp in the SVG implementation in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the resizing of a view.
CVE-2013-6664	Use-after-free vulnerability in the FormAssociatedElement::formRemovedFromTree function in core/html/FormAssociatedElement.cpp in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving FORM elements, as demonstrated by use of the speech-recognition feature.
CVE-2013-6665	Heap-based buffer overflow in the ResourceProvider::InitializeSoftware function in cc/resources/resource_provider.cc in Google Chrome before 33.0.1750.146 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large texture size that triggers improper memory allocation in the software renderer.

CVE-2013-6666	The PepperFlashRendererHost::OnNavigate function in renderer/pepper/pepper_flash_renderer_host.cc in Google Chrome before 33.0.1750.146 does not verify that all headers are Cross-Origin Resource Sharing (CORS) simple headers before proceeding with a PPB_Flash.Navigate operation, which might allow remote attackers to bypass intended CORS restrictions via an inappropriate header.
CVE-2013-6667	Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.146 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6668	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.10, as used in Google Chrome before 33.0.1750.146, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6802	Google Chrome before 31.0.1650.57 allows remote attackers to bypass intended sandbox restrictions by leveraging access to a renderer process, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013, a different vulnerability than CVE-2013-6632.
CVE-2013-6916	Cross-site scripting (XSS) vulnerability in the Yahoo! User Interface Library in Cybozu Garoon before 3.7.2, when Internet Explorer 9 or 10 or Chrome is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2014-1681	Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.102 have unknown impact and attack vectors, related to 12 "security fixes [that were not] either contributed by external researchers or particularly interesting."
CVE-2014-1700	Use-after-free vulnerability in modules/speech/SpeechSynthesis.cpp in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of a certain utterance data structure.
CVE-2014-1701	The GenerateFunction function in bindings/scripts/code_generator_v8.pm in Blink, as used in Google Chrome before 33.0.1750.149, does not implement a certain cross-origin restriction for the EventTarget::dispatchEvent function, which allows remote attackers to conduct Universal XSS (UXSS) attacks via vectors involving events.
CVE-2014-1702	Use-after-free vulnerability in the DatabaseThread::cleanupDatabaseThread function in modules/webdatabase/DatabaseThread.cpp in the web database implementation in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of scheduled tasks during shutdown of a thread.
CVE-2014-1703	Use-after-free vulnerability in the WebSocketDispatcherHost::SendOrDrop function in content/browser/renderer_host/websocket_dispatcher_host.cc in the Web Sockets implementation in Google Chrome before 33.0.1750.149 might allow remote attackers to bypass the sandbox protection mechanism by leveraging an incorrect deletion in a certain failure case.
CVE-2014-1704	Multiple unspecified vulnerabilities in Google V8 before 3.23.17.18, as used in Google Chrome before 33.0.1750.149, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1705	Google V8, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2014-1713	Use-after-free vulnerability in the AttributeSetter function in bindings/templates/attributes.cpp in the bindings in Blink, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the document.location value.
CVE-2014-1714	The ScopedClipboardWriter::WritePickledData function in ui/base/clipboard/scoped_clipboard_writer.cc in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows does not verify a certain format value, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the clipboard.
CVE-2014-1715	Directory traversal vulnerability in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows has unspecified impact and attack vectors.
CVE-2014-1716	Cross-site scripting (XSS) vulnerability in the Runtime_SetPrototype function in runtime.cc in Google V8, as used in Google Chrome before 34.0.1847.116, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Universal XSS (UXSS)."
CVE-2014-1717	Google V8, as used in Google Chrome before 34.0.1847.116, does not properly use numeric casts during handling of typed arrays, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2014-1718	Integer overflow in the SoftwareFrameManager::SwapToNewFrame function in content/browser/renderer_host/software_frame_manager.cc in the software compositor in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted mapping of a large amount of renderer memory.
CVE-2014-1719	Use-after-free vulnerability in the WebSharedWorkerStub::OnTerminateWorkerContext function in content/worker/websharedworker_stub.cc in the Web Workers implementation in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger a SharedWorker termination during script loading.

CVE-2014-1720	Use-after-free vulnerability in the HTMLBodyElement::insertedInto function in core/html/HTMLBodyElement.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attributes.
CVE-2014-1721	Google V8, as used in Google Chrome before 34.0.1847.116, does not properly implement lazy deoptimization, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by improper handling of a heap allocation of a number outside the Small Integer (aka smi) range.
CVE-2014-1722	Use-after-free vulnerability in the RenderBlock::addChildIgnoringAnonymousColumnBlocks function in core/rendering/RenderBlock.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving addition of a child node.
CVE-2014-1723	The UnescapeURLWithOffsetsImpl function in net/base/escape.cc in Google Chrome before 34.0.1847.116 does not properly handle bidirectional Internationalized Resource Identifiers (IRIs), which makes it easier for remote attackers to spoof URLs via crafted use of right-to-left (RTL) Unicode text.
CVE-2014-1724	Use-after-free vulnerability in Free(b)soft Laboratory Speech Dispatcher 0.7.1, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service (application hang) or possibly have unspecified other impact via a text-to-speech request.
CVE-2014-1725	The base64DecodeInternal function in wtf/text/Base64.cpp in Blink, as used in Google Chrome before 34.0.1847.116, does not properly handle string data composed exclusively of whitespace characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via a window.atob method call.
CVE-2014-1726	The drag implementation in Google Chrome before 34.0.1847.116 allows user-assisted remote attackers to bypass the Same Origin Policy and forge local pathnames by leveraging renderer access.
CVE-2014-1727	Use-after-free vulnerability in content/renderer/renderer_webcolorchooser_impl.h in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to forms.
CVE-2014-1728	Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1729	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.22, as used in Google Chrome before 34.0.1847.116, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1730	Google V8, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly store internationalization metadata, which allows remote attackers to bypass intended access restrictions by leveraging "type confusion" and reading property values, related to i18n.js and runtime.cc.
CVE-2014-1731	core/html/HTMLSelectElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly check renderer state upon a focus event, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion" for SELECT elements.
CVE-2014-1732	Use-after-free vulnerability in browser/ui/views/speech_recognition_bubble_views.cc in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via an INPUT element that triggers the presence of a Speech Recognition Bubble window for an incorrect duration.
CVE-2014-1733	The PointerCompare function in codegen.cc in Seccomp-BPF, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly merge blocks, which might allow remote attackers to bypass intended sandbox restrictions by leveraging renderer access.
CVE-2014-1734	Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1735	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.33, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1736	Integer overflow in api.cc in Google V8, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value.
CVE-2014-1740	Multiple use-after-free vulnerabilities in net/websockets/websocket_job.cc in the WebSockets implementation in Google Chrome before 34.0.1847.137 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to WebSocketJob deletion.
CVE-2014-1741	Multiple integer overflows in the replace-data functionality in the CharacterData interface implementation in core/dom/CharacterData.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to ranges.
CVE-2014-1742	Use-after-free vulnerability in the FrameSelection::updateAppearance function in core/editing/FrameSelection.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper RenderObject handling.

CVE-2014-1743	Use-after-free vulnerability in the StyleElement::removedFromDocument function in core/dom/StyleElement.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that triggers tree mutation.
CVE-2014-1744	Integer overflow in the AudioInputRendererHost::OnCreateStream function in content/browser/renderer_host/media/audio_input_renderer_host.cc in Google Chrome before 35.0.1916.114 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a large shared-memory allocation.
CVE-2014-1745	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger removal of an SVGFontFaceElement object, related to core/svg/SVGFontFaceElement.cpp.
CVE-2014-1746	The InMemoryUrlProtocol::Read function in media/filters/in_memory_url_protocol.cc in Google Chrome before 35.0.1916.114 relies on an insufficiently large integer data type, which allows remote attackers to cause a denial of service (out-of-bounds read) via vectors that trigger use of a large buffer.
CVE-2014-1747	Cross-site scripting (XSS) vulnerability in the DocumentLoader::maybeCreateArchive function in core/loader/DocumentLoader.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to inject arbitrary web script or HTML via crafted MHTML content, aka "Universal XSS (UXSS)."
CVE-2014-1748	The ScrollView::paint function in platform/scroll/ScrollView.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to spoof the UI by extending scrollbar painting into the parent frame.
CVE-2014-1749	Multiple unspecified vulnerabilities in Google Chrome before 35.0.1916.114 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3152	Integer underflow in the LCodeGen::PrepareKeyedOperand function in arm/lithium-codegen-arm.cc in Google V8 before 3.25.28.16, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a negative key value.
CVE-2014-3154	Use-after-free vulnerability in the ChildThread::Shutdown function in content/child/child_thread.cc in the filesystem API in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to a Blink shutdown.
CVE-2014-3155	net/spdy/spdy_write_queue.cc in the SPDY implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging incorrect queue maintenance.
CVE-2014-3156	Buffer overflow in the clipboard implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unexpected bitmap data, related to content/renderer/renderer_clipboard_client.cc and content/renderer/webclipboard_impl.cc.
CVE-2014-3157	Heap-based buffer overflow in the FFmpegVideoDecoder::GetVideoBuffer function in media/filters/ffmpeg_video_decoder.cc in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging VideoFrame data structures that are too small for proper interaction with an underlying FFmpeg library.
CVE-2014-3159	The WebContentsDelegateAndroid::OpenURLFromTab function in components/web_contents_delegate_android/web_contents_delegate_android.cc in Google Chrome before 36.0.1985.122 on Android does not properly restrict URL loading, which allows remote attackers to spoof the URL in the Omnibox via unspecified vectors.
CVE-2014-3160	The ResourceFetcher::canRequest function in core/fetch/ResourceFetcher.cpp in Blink, as used in Google Chrome before 36.0.1985.125, does not properly restrict subresource requests associated with SVG files, which allows remote attackers to bypass the Same Origin Policy via a crafted file.
CVE-2014-3161	The WebMediaPlayerAndroid::load function in content/renderer/media/android/webmediaplayer_android.cc in Google Chrome before 36.0.1985.122 on Android does not properly interact with redirects, which allows remote attackers to bypass the Same Origin Policy via a crafted web site that hosts a video stream.
CVE-2014-3162	Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.125 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3165	Use-after-free vulnerability in modules/websockets/WorkerThreadableWebSocketChannel.cpp in the Web Sockets implementation in Blink, as used in Google Chrome before 36.0.1985.143, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an unexpectedly long lifetime of a temporary object during method completion.
CVE-2014-3166	The Public Key Pinning (PKP) implementation in Google Chrome before 36.0.1985.143 on Windows, OS X, and Linux, and before 36.0.1985.135 on Android, does not correctly consider the properties of SPDY connections, which allows remote attackers to obtain sensitive information by leveraging the use of multiple domain names.
CVE-2014-3167	Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.143 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3168	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper caching associated with animation.

CVE-2014-3169	Use-after-free vulnerability in core/dom/ContainerNode.cpp in the DOM implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging script execution that occurs before notification of node removal.
CVE-2014-3170	extensions/common/url_pattern.cc in Google Chrome before 37.0.2062.94 does not prevent use of a '\0' character in a host name, which allows remote attackers to spoof the extension permission dialog by relying on truncation after this character.
CVE-2014-3171	Use-after-free vulnerability in the V8 bindings in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper use of HashMap add operations instead of HashMap set operations, related to bindings/core/v8/DOMWrapperMap.h and bindings/core/v8/SerializedScriptValue.cpp.
CVE-2014-3172	The Debugger extension API in browser/extensions/api/debugger/debugger_api.cc in Google Chrome before 37.0.2062.94 does not validate a tab's URL before an attach operation, which allows remote attackers to bypass intended access limitations via an extension that uses a restricted URL, as demonstrated by a chrome:// URL.
CVE-2014-3173	The WebGL implementation in Google Chrome before 37.0.2062.94 does not ensure that clear calls interact properly with the state of a draw buffer, which allows remote attackers to cause a denial of service (read of uninitialized memory) via a crafted CANVAS element, related to gpu/command_buffer/service/framebuffer_manager.cc and gpu/command_buffer/service/gles2_cmd_decoder.cc.
CVE-2014-3174	modules/webaudio/BiquadDSPKernel.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 37.0.2062.94, does not properly consider concurrent threads during attempts to update biquad filter coefficients, which allows remote attackers to cause a denial of service (read of uninitialized memory) via crafted API calls.
CVE-2014-3175	Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.94 allow attackers to cause a denial of service or possibly have other impact via unknown vectors, related to the load_truetype_glyph function in truetype/ttload.c in FreeType and other functions in other components.
CVE-2014-3176	Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3177.
CVE-2014-3177	Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3176.
CVE-2014-3178	Use-after-free vulnerability in core/dom/Node.cpp in Blink, as used in Google Chrome before 37.0.2062.120, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of render-tree inconsistencies.
CVE-2014-3179	Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.120 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3187	Google Chrome before 37.0.2062.60 and 38.x before 38.0.2125.59 on iOS does not properly restrict processing of (1) facetime:// and (2) facetime-audio:// URLs, which allows remote attackers to obtain video and audio data from a device via a crafted web site.
CVE-2014-3188	Google Chrome before 38.0.2125.101 and Chrome OS before 38.0.2125.101 do not properly handle the interaction of IPC and Google V8, which allows remote attackers to execute arbitrary code via vectors involving JSON data, related to improper parsing of an escaped index by ParseJsonObject in json-parser.h.
CVE-2014-3189	The chrome_pdf::CopyImage function in pdf/draw_utils.cc in the PDFium component in Google Chrome before 38.0.2125.101 does not properly validate image-data dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via unknown vectors.
CVE-2014-3190	Use-after-free vulnerability in the Event::currentTarget function in core/events/Event.cpp in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that accesses the path property of an Event object.
CVE-2014-3191	Use-after-free vulnerability in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers a widget-position update that improperly interacts with the render tree, related to the FrameView::updateLayoutAndStyleForPainting function in core/frame/FrameView.cpp and the RenderLayerScrollableArea::setScrollOffset function in core/rendering/RenderLayerScrollableArea.cpp.
CVE-2014-3192	Use-after-free vulnerability in the ProcessingInstruction::setXSLStyleSheet function in core/dom/ProcessingInstruction.cpp in the DOM implementation in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3193	The SessionService::GetLastSession function in browser/sessions/session_service.cc in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors that leverage "type confusion" for callback processing.

CVE-2014-3194	Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3195	Google V8, as used in Google Chrome before 38.0.2125.101, does not properly track JavaScript heap-memory allocations as allocations of uninitialized memory and does not properly concatenate arrays of double-precision floating-point numbers, which allows remote attackers to obtain sensitive information via crafted JavaScript code, related to the PagedSpace::AllocateRaw and NewSpace::AllocateRaw functions in heap/spaces-inl.h, the LargeObjectSpace::AllocateRaw function in heap/spaces.cc, and the Runtime_ArrayConcat function in runtime.cc.
CVE-2014-3196	base/memory/shared_memory_win.cc in Google Chrome before 38.0.2125.101 on Windows does not properly implement read-only restrictions on shared memory, which allows attackers to bypass a sandbox protection mechanism via unspecified vectors.
CVE-2014-3197	The NavigationScheduler::schedulePageBlock function in core/loader/NavigationScheduler.cpp in Blink, as used in Google Chrome before 38.0.2125.101, does not properly provide substitute data for pages blocked by the XSS auditor, which allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2014-3198	The Instance::HandleInputEvent function in pdf/instance.cc in the PDFium component in Google Chrome before 38.0.2125.101 interprets a certain -1 value as an index instead of a no-visible-page error code, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-3199	The wrap function in bindings/core/v8/custom/V8EventCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 38.0.2125.101, has an erroneous fallback outcome for wrapper-selection failures, which allows remote attackers to cause a denial of service via vectors that trigger stopping a worker process that had been handling an Event object.
CVE-2014-3200	Multiple unspecified vulnerabilities in Google Chrome before 38.0.2125.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3201	core/rendering/compositing/RenderLayerCompositor.cpp in Blink, as used in Google Chrome before 38.0.2125.102 on Android, does not properly handle a certain IFRAME overflow condition, which allows remote attackers to spoof content via a crafted web site that interferes with the scrollbar.
CVE-2014-3803	The SpeechInput feature in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to enable microphone access and obtain speech-recognition text without indication via an INPUT element with a -webkit-speech attribute.
CVE-2014-6160	IBM WebSphere Service Registry and Repository (WSRR) 8.5 before 8.5.0.1, when Chrome and WebSEAL are used, does not properly process ServiceRegistryDashboard logout actions, which allows remote attackers to bypass intended access restrictions by leveraging an unattended workstation.
CVE-2014-7899	Google Chrome before 38.0.2125.101 allows remote attackers to spoof the address bar by placing a blob: substring at the beginning of the URL, followed by the original URI scheme and a long username string.
CVE-2014-7900	Use-after-free vulnerability in the CPDF_Parser::IsLinearizedFile function in fpdfapi/fpdf_parser/fpdf_parser.cpp in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7901	Integer overflow in the opj_t2_read_packet_data function in fxcodec/fx_libopenjpeg/libopenjpeg20/t2.c in OpenJPEG in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long segment in a JPEG image.
CVE-2014-7902	Use-after-free vulnerability in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7903	Buffer overflow in OpenJPEG before r2911 in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JPEG image.
CVE-2014-7904	Buffer overflow in Skia, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7905	Google Chrome before 39.0.2171.65 on Android does not prevent navigation to a URL in cases where an intent for the URL lacks CATEGORY_BROWSABLE, which allows remote attackers to bypass intended access restrictions via a crafted web site.
CVE-2014-7906	Use-after-free vulnerability in the Pepper plugins in Google Chrome before 39.0.2171.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Flash content that triggers an attempted PepperMediaDeviceManager access outside of the object's lifetime.
CVE-2014-7907	Multiple use-after-free vulnerabilities in modules/screen_orientation/ScreenOrientationController.cpp in Blink, as used in Google Chrome before 39.0.2171.65, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger improper handling of a detached frame, related to the (1) lock and (2) unlock methods.
CVE-2014-7908	Multiple integer overflows in the CheckMov function in media/base/container_names.cc in Google Chrome before 39.0.2171.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a large atom in (1) MPEG-4 or (2) QuickTime .mov data.
CVE-2014-7909	effects/SkDashPathEffect.cpp in Skia, as used in Google Chrome before 39.0.2171.65, computes a hash key using uninitialized integer values, which might allow remote attackers to cause a denial of service by rendering crafted data.

CVE-2014-7910	Multiple unspecified vulnerabilities in Google Chrome before 39.0.2171.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-7923	The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors related to a (1) zero-length quantifier or (2) look-behind expression, a different vulnerability than CVE-2014-7926.
CVE-2014-7924	Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering duplicate BLOB references, related to content/browser/indexed_db/indexed_db_callbacks.cc and content/browser/indexed_db/indexed_db_dispatcher_host.cc.
CVE-2014-7925	Use-after-free vulnerability in the WebAudio implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an audio-rendering thread in which AudioNode data is improperly maintained.
CVE-2014-7926	The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors related to a (1) zero-length quantifier or (2) look-behind expression, a different vulnerability than CVE-2014-7923.
CVE-2014-7927	The SimplifiedLowering::DoLoadBuffer function in compiler/simplified-lowering.cc in Google V8, as used in Google Chrome before 40.0.2214.91, does not properly choose an integer data type, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2014-7928	hydrogen.cc in Google V8, as used Google Chrome before 40.0.2214.91, does not properly handle arrays with holes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers an array copy.
CVE-2014-7929	Use-after-free vulnerability in the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving movement of a SCRIPT element across documents.
CVE-2014-7930	Use-after-free vulnerability in core/events/TreeScopeEventContext.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers improper maintenance of TreeScope data.
CVE-2014-7931	factory.cc in Google V8, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers improper maintenance of backing-store pointers.
CVE-2014-7932	Use-after-free vulnerability in the Element::detach function in core/dom/Element.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving pending updates of detached elements.
CVE-2014-7933	Use-after-free vulnerability in the matroska_read_seek function in libavformat/matroskadec.c in FFmpeg before 2.5.1, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska file that triggers improper maintenance of tracks data.
CVE-2014-7934	Use-after-free vulnerability in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to unexpected absence of document data structures.
CVE-2014-7935	Use-after-free vulnerability in browser/speech/tts_message_filter.cc in the Speech implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving utterances from a closed tab.
CVE-2014-7936	Use-after-free vulnerability in the ZoomBubbleView::Close function in browser/ui/views/location_bar/zoom_bubble_view.cc in the Views implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that triggers improper maintenance of a zoom bubble.
CVE-2014-7937	Multiple off-by-one errors in libavcodec/vorbisdec.c in FFmpeg before 2.4.2, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Vorbis I data.
CVE-2014-7938	The Fonts implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2014-7939	Google Chrome before 40.0.2214.91, when the Harmony proxy in Google V8 is enabled, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code with Proxy.create and console.log calls, related to HTTP responses that lack an "X-Content-Type-Options: nosniff" header.
CVE-2014-7940	The collator implementation in i18n/ucol.cpp in International Components for Unicode (ICU) 52 through SVN revision 293126, as used in Google Chrome before 40.0.2214.91, does not initialize memory for a data structure,

	which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted character sequence.
CVE-2014-7941	The SelectionOwner::ProcessTarget function in ui/base/x/selection_owner.cc in the UI implementation in Google Chrome before 40.0.2214.91 uses an incorrect data type for a certain length value, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted X11 data.
CVE-2014-7942	The Fonts implementation in Google Chrome before 40.0.2214.91 does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7943	Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-7944	The sycc422_to_rgb function in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 40.0.2214.91, does not properly handle odd values of image width, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2014-7945	OpenJPEG before r2908, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, and t2.c.
CVE-2014-7946	The RenderTable::simplifiedNormalFlowLayout function in core/rendering/RenderTable.cpp in Blink, as used in Google Chrome before 40.0.2214.91, skips captions during table layout in certain situations, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors related to the Fonts implementation.
CVE-2014-7947	OpenJPEG before r2944, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, pi.c, t1.c, t2.c, and tcd.c.
CVE-2014-7948	The AppCacheUpdateJob::URLFetcher::OnResponseStarted function in content/browser/appcache/appcache_update_job.cc in Google Chrome before 40.0.2214.91 proceeds with AppCache caching for SSL sessions even if there is an X.509 certificate error, which allows man-in-the-middle attackers to spoof HTML5 application content via a crafted certificate.
CVE-2014-7967	Multiple unspecified vulnerabilities in Google V8 before 3.28.71.15, as used in Google Chrome before 38.0.2125.101, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-9646	Unquoted Windows search path vulnerability in the GoogleChromeDistribution::DoPostUninstallOperations function in installer/util/google_chrome_distribution.cc in the uninstall-survey feature in Google Chrome before 40.0.2214.91 allows local users to gain privileges via a Trojan horse program in the %SYSTEMDRIVE% directory, as demonstrated by program.exe, a different vulnerability than CVE-2015-1205.
CVE-2014-9647	Use-after-free vulnerability in PDFium, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/src/fpdfview.cpp and fpdfsdk/src/fsdk_mgr.cpp, a different vulnerability than CVE-2015-1205.
CVE-2014-9648	components/navigation_interception/intercept_navigation_resource_throttle.cc in Google Chrome before 40.0.2214.91 on Android does not properly restrict use of intent: URLs to open an application after navigation to a web site, which allows remote attackers to cause a denial of service (loss of browser access to that site) via crafted JavaScript code, as demonstrated by pandora.com and the Pandora application, a different vulnerability than CVE-2015-1205.
CVE-2014-9689	content/renderer/device_sensors/device_orientation_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate gyroscope data, which makes it easier for remote attackers to obtain speech signals from a device's physical environment via a crafted web site that listens for ondeviceorientation events, a different vulnerability than CVE-2015-1231.
CVE-2015-1205	Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.91 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1209	Use-after-free vulnerability in the VisibleSelection::nonBoundaryShadowTreeRootNode function in core/editing/VisibleSelection.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers improper handling of a shadow-root anchor.
CVE-2015-1210	The V8ThrowException::createDOMException function in bindings/core/v8/V8ThrowException.cpp in the V8 bindings in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, does not properly consider frame access restrictions during the throwing of an exception, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2015-1211	The OriginCanAccessServiceWorkers function in content/browser/service_worker/service_worker_dispatcher_host.cc in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android does not properly restrict the URI scheme during a ServiceWorker registration, which allows remote attackers to gain privileges via a filesystem: URI.

CVE-2015-1212	Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1213	The SkBitmap::ReadRawPixels function in core/SkBitmap.cpp in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation.
CVE-2015-1214	Integer overflow in the SkAutoSTArray implementation in include/core/SkTemplates.h in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a reset action with a large count value, leading to an out-of-bounds write operation.
CVE-2015-1215	The filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation.
CVE-2015-1216	Use-after-free vulnerability in the V8Window::namedPropertyGetterCustom function in bindings/core/v8/custom/V8WindowCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a frame detachment.
CVE-2015-1217	The V8LazyEventListener::prepareListenerObject function in bindings/core/v8/V8LazyEventListener.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, does not properly compile listeners, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-1218	Multiple use-after-free vulnerabilities in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger movement of a SCRIPT element to different documents, related to (1) the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp and (2) the SVGScriptElement::didMoveToNewDocument function in core/svg/SVGScriptElement.cpp.
CVE-2015-1219	Integer overflow in the SkMallocPixelRef::NewAllocate function in core/SkMallocPixelRef.cpp in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted allocation of a large amount of memory during WebGL rendering.
CVE-2015-1220	Use-after-free vulnerability in the GIFImageReader::parseData function in platform/image-decoders/gif/GIFImageReader.cpp in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted frame size in a GIF image.
CVE-2015-1221	Use-after-free vulnerability in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect ordering of operations in the Web SQL Database thread relative to Blink's main thread, related to the shutdown function in web/WebKit.cpp.
CVE-2015-1222	Multiple use-after-free vulnerabilities in the ServiceWorkerScriptCacheMap implementation in content/browser/service_worker/service_worker_script_cache_map.cc in Google Chrome before 41.0.2272.76 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a ServiceWorkerContextWrapper::DeleteAndStartOver call, related to the NotifyStartedCaching and NotifyFinishedCaching functions.
CVE-2015-1223	Multiple use-after-free vulnerabilities in core/html/HTMLInputElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger extraneous change events, as demonstrated by events for invalid input or input to read-only fields, related to the initializeTypeInParsing and updateType functions.
CVE-2015-1224	The VpxVideoDecoder::VpxDecode function in media/filters/vpx_video_decoder.cc in the vpxdecoder implementation in Google Chrome before 41.0.2272.76 does not ensure that alpha-plane dimensions are identical to image dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted VPx video data.
CVE-2015-1225	PDFium, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-1226	The DebuggerFunction::InitAgentHost function in browser/extensions/api/debugger/debugger_api.cc in Google Chrome before 41.0.2272.76 does not properly restrict what URLs are available as debugger targets, which allows remote attackers to bypass intended access restrictions via a crafted extension.
CVE-2015-1227	The DragImage::create function in platform/DragImage.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not initialize memory for image drawing, which allows remote attackers to have an unspecified impact by triggering a failed image decoding, as demonstrated by an image for which the default orientation cannot be used.
CVE-2015-1228	The RenderCounter::updateCounter function in core/rendering/RenderCounter.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not force a relayout operation and consequently does not initialize memory for a

	<p>data structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted Cascading Style Sheets (CSS) token sequence.</p>
CVE-2015-1229	net/http/proxy_client_socket.cc in Google Chrome before 41.0.2272.76 does not properly handle a 407 (aka Proxy Authentication Required) HTTP status code accompanied by a Set-Cookie header, which allows remote proxy servers to conduct cookie-injection attacks via a crafted response.
CVE-2015-1230	The getHiddenProperty function in bindings/core/v8/V8EventListenerList.h in Blink, as used in Google Chrome before 41.0.2272.76, has a name conflict with the AudioContext class, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that adds an AudioContext event listener and triggers "type confusion."
CVE-2015-1231	Multiple unspecified vulnerabilities in Google Chrome before 41.0.2272.76 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1232	Array index error in the MidiManagerUsb::DispatchSendMidiData function in media/midi/midi_manager_usb.cc in Google Chrome before 41.0.2272.76 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging renderer access to provide an invalid port index that triggers an out-of-bounds write operation, a different vulnerability than CVE-2015-1212.
CVE-2015-1233	Google Chrome before 41.0.2272.118 does not properly handle the interaction of IPC, the Gamepad API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2015-1234	Race condition in gpu/command_buffer/service/gles2_cmd_decoder.cc in Google Chrome before 41.0.2272.118 allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact by manipulating OpenGL ES commands.
CVE-2015-1235	The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in the HTML parser in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy via a crafted HTML document with an IFRAME element.
CVE-2015-1236	The MediaElementAudioSourceNode::process function in modules/webaudio/MediaElementAudioSourceNode.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy and obtain sensitive audio sample values via a crafted web site containing a media element.
CVE-2015-1237	Use-after-free vulnerability in the RenderFrameImpl::OnMessageReceived function in content/renderer/render_frame_impl.cc in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger renderer IPC messages during a detach operation.
CVE-2015-1238	Skia, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.
CVE-2015-1240	gpu/blink/webgraphicscontext3d_impl.cc in the WebGL implementation in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebGL program that triggers a state inconsistency.
CVE-2015-1241	Google Chrome before 42.0.2311.90 does not properly consider the interaction of page navigation with the handling of touch events and gesture events, which allows remote attackers to trigger unintended UI actions via a crafted web site that conducts a "tapjacking" attack.
CVE-2015-1242	The ReduceTransitionElementsKind function in hydrogen-check-elimination.cc in Google V8 before 4.2.77.8, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that leverages "type confusion" in the check-elimination optimization.
CVE-2015-1243	Use-after-free vulnerability in the MutationObserver::disconnect function in core/dom/MutationObserver.cpp in the DOM implementation in Blink, as used in Google Chrome before 42.0.2311.135, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an attempt to unregister a MutationObserver object that is not currently registered.
CVE-2015-1244	The URLRequest::GetHSTSRedirect function in url_request/url_request.cc in Google Chrome before 42.0.2311.90 does not replace the ws scheme with the wss scheme whenever an HSTS Policy is active, which makes it easier for remote attackers to obtain sensitive information by sniffing the network for WebSocket traffic.
CVE-2015-1245	Use-after-free vulnerability in the OpenPDFInReaderView::Update function in browser/ui/views/location_bar/open_pdf_in_reader_view.cc in Google Chrome before 41.0.2272.76 might allow user-assisted remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering interaction with a PDFium "Open PDF in Reader" button that has an invalid tab association.
CVE-2015-1246	Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-1247	The SearchEngineTabHelper::OnPageHasOSDD function in browser/ui/search_engines/search_engine_tab_helper.cc in Google Chrome before 42.0.2311.90 does not prevent use of a file: URL for an OpenSearch descriptor XML document, which might allow remote attackers to obtain sensitive information from local files via a crafted (1) http or (2) https web site.

CVE-2015-1248	The FileSystem API in Google Chrome before 40.0.2214.91 allows remote attackers to bypass the SafeBrowsing for Executable Files protection mechanism by creating a .exe file in a temporary filesystem and then referencing this file with a filesystem: <code>http://</code> URL.
CVE-2015-1249	Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.90 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1250	Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.135 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1251	Use-after-free vulnerability in the SpeechRecognitionClient implementation in the Speech subsystem in Google Chrome before 43.0.2357.65 allows remote attackers to execute arbitrary code via a crafted document.
CVE-2015-1252	common/partial_circular_buffer.cc in Google Chrome before 43.0.2357.65 does not properly handle wraps, which allows remote attackers to bypass a sandbox protection mechanism or cause a denial of service (out-of-bounds write) via vectors that trigger a write operation with a large amount of data, related to the PartialCircularBuffer::Write and PartialCircularBuffer::DoWrite functions.
CVE-2015-1253	core/html/parser/HTMLConstructionSite.cpp in the DOM implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that appends a child to a SCRIPT element, related to the insert and executeReparentTask functions.
CVE-2015-1254	core/dom/Document.cpp in Blink, as used in Google Chrome before 43.0.2357.65, enables the inheritance of the designMode attribute, which allows remote attackers to bypass the Same Origin Policy by leveraging the availability of editing.
CVE-2015-1255	Use-after-free vulnerability in content/renderer/media/webaudio_capturer_source.cc in the WebAudio implementation in Google Chrome before 43.0.2357.65 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging improper handling of a stop action for an audio track.
CVE-2015-1256	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that leverages improper handling of a shadow tree for a use element.
CVE-2015-1257	platform/graphics/filters/FECColorMatrix.cpp in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, does not properly handle an insufficient number of values in an feColorMatrix filter, which allows remote attackers to cause a denial of service (container overflow) or possibly have unspecified other impact via a crafted document.
CVE-2015-1258	Google Chrome before 43.0.2357.65 relies on libvpx code that was not built with an appropriate --size-limit value, which allows remote attackers to trigger a negative value for a size field, and consequently cause a denial of service or possibly have unspecified other impact, via a crafted frame size in VP9 video data.
CVE-2015-1259	PDFium, as used in Google Chrome before 43.0.2357.65, does not properly initialize memory, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2015-1260	Multiple use-after-free vulnerabilities in content/renderer/media/user_media_client_impl.cc in the WebRTC implementation in Google Chrome before 43.0.2357.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that executes upon completion of a getUserMedia request.
CVE-2015-1261	android/java/src/org/chromium/chrome/browser/WebsiteSettingsPopup.java in Google Chrome before 43.0.2357.65 on Android does not properly restrict use of a URL's fragment identifier during construction of a page-info popup, which allows remote attackers to spoof the URL bar or deliver misleading popup content via crafted text.
CVE-2015-1262	platform/fonts/shaping/HarfBuzzShaper.cpp in Blink, as used in Google Chrome before 43.0.2357.65, does not initialize a certain width field, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Unicode text.
CVE-2015-1263	The Spellcheck API implementation in Google Chrome before 43.0.2357.65 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file.
CVE-2015-1264	Cross-site scripting (XSS) vulnerability in Google Chrome before 43.0.2357.65 allows user-assisted remote attackers to inject arbitrary web script or HTML via crafted data that is improperly handled by the Bookmarks feature.
CVE-2015-1265	Multiple unspecified vulnerabilities in Google Chrome before 43.0.2357.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1266	content/browser/webui/content_web_ui_controller_factory.cc in Google Chrome before 43.0.2357.130 does not properly consider the scheme in determining whether a URL is associated with a WebUI SiteInstance, which allows remote attackers to bypass intended access restrictions via a similar URL, as demonstrated by use of <code>http://gpu</code> when there is a WebUI class for handling <code>chrome://gpu</code> requests.
CVE-2015-1267	Blink, as used in Google Chrome before 43.0.2357.130, does not properly restrict the creation context during creation of a DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that uses a Blink public API, related to <code>WebArrayBufferConverter.cpp</code> , <code>WebBlob.cpp</code> , <code>WebDOMError.cpp</code> , and <code>WebDOMFileSystem.cpp</code> .

CVE-2015-1268	bindings/scripts/v8_types.py in Blink, as used in Google Chrome before 43.0.2357.130, does not properly select a creation context for a return value's DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code, as demonstrated by use of a data: URL.
CVE-2015-1269	The DecodeHSTSPreloadRaw function in net/http/transport_security_state.cc in Google Chrome before 43.0.2357.130 does not properly canonicalize DNS hostnames before making comparisons to HSTS or HPKP preload entries, which allows remote attackers to bypass intended access restrictions via a string that (1) ends in a . (dot) character or (2) is not entirely lowercase.
CVE-2015-1270	The ucnv_io_getConverterName function in common/ucnv_io.cpp in International Components for Unicode (ICU), as used in Google Chrome before 44.0.2403.89, mishandles converter names with initial x- substrings, which allows remote attackers to cause a denial of service (read of uninitialized memory) or possibly have unspecified other impact via a crafted file.
CVE-2015-1271	PDFium, as used in Google Chrome before 44.0.2403.89, does not properly handle certain out-of-memory conditions, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted PDF document that triggers a large memory allocation.
CVE-2015-1272	Use-after-free vulnerability in the GPU process implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the continued availability of a GPUChannelHost data structure during Blink shutdown, related to content/browser/gpu/browser_gpu_channel_host_factory.cc and content/renderer/render_thread_impl.cc.
CVE-2015-1273	Heap-based buffer overflow in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service or possibly have unspecified other impact via invalid JPEG2000 data in a PDF document.
CVE-2015-1274	Google Chrome before 44.0.2403.89 does not ensure that the auto-open list omits all dangerous file types, which makes it easier for remote attackers to execute arbitrary code by providing a crafted file and leveraging a user's previous "Always open files of this type" choice, related to download_commands.cc and download_prefs.cc.
CVE-2015-1275	Cross-site scripting (XSS) vulnerability in org/chromium/chrome/browser/UrlUtilities.java in Google Chrome before 44.0.2403.89 on Android allows remote attackers to inject arbitrary web script or HTML via a crafted intent: URL, as demonstrated by a trailing alert(document.cookie);// substring, aka "Universal XSS (UXSS)."
CVE-2015-1276	Use-after-free vulnerability in content/browser/indexed_db/indexed_db_backing_store.cc in the IndexedDB implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an abort action before a certain write operation.
CVE-2015-1277	Use-after-free vulnerability in the accessibility implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging lack of certain validity checks for accessibility-tree data structures.
CVE-2015-1278	content/browser/web_contents/web_contents_impl.cc in Google Chrome before 44.0.2403.89 does not ensure that a PDF document's modal dialog is closed upon navigation to an interstitial page, which allows remote attackers to spoof URLs via a crafted document, as demonstrated by the alert_dialog.pdf document.
CVE-2015-1279	Integer overflow in the CJBIG2_Image::expand function in fxcodect/jbig2/JBIG2_Image.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via large height and stride values.
CVE-2015-1280	SkPictureShader.cpp in Skia, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging access to a renderer process and providing crafted serialized data.
CVE-2015-1281	core/loader/ImageLoader.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly determine the V8 context of a microtask, which allows remote attackers to bypass Content Security Policy (CSP) restrictions by providing an image from an unintended source.
CVE-2015-1282	Multiple use-after-free vulnerabilities in fpdfsdk/src/javascript/Document.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to the (1) Document::delay and (2) Document::DoFieldDelay functions.
CVE-2015-1283	Multiple integer overflows in the XML_GetBuffer function in Expat through 2.1.0, as used in Google Chrome before 44.0.2403.89 and other products, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted XML data, a related issue to CVE-2015-2716.
CVE-2015-1284	The LocalFrame::isURLAllowed function in core/frame/LocalFrame.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly check for a page's maximum number of frames, which allows remote attackers to cause a denial of service (invalid count value and use-after-free) or possibly have unspecified other impact via crafted JavaScript code that makes many createElement calls for IFRAME elements.
CVE-2015-1285	The XSSAuditor::canonicalize function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 44.0.2403.89, does not properly choose a truncation point, which makes it easier for remote attackers to obtain sensitive information via an unspecified linear-time attack.
CVE-2015-1286	Cross-site scripting (XSS) vulnerability in the V8ContextNativeHandler::GetModuleSystem function in extensions/renderer/v8_context_native_handler.cc in Google Chrome before 44.0.2403.89 allows remote attackers

	to inject arbitrary web script or HTML by leveraging the lack of a certain V8 context restriction, aka a Blink "Universal XSS (UXSS)."
CVE-2015-1287	Blink, as used in Google Chrome before 44.0.2403.89, enables a quirks-mode exception that limits the cases in which a Cascading Style Sheets (CSS) document is required to have the text/css content type, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, related to core/fetch/CSSStyleSheetResource.cpp.
CVE-2015-1288	The Spellcheck API implementation in Google Chrome before 44.0.2403.89 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file, a related issue to CVE-2015-1263.
CVE-2015-1289	Multiple unspecified vulnerabilities in Google Chrome before 44.0.2403.89 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1291	The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not check whether a node is expected, which allows remote attackers to bypass the Same Origin Policy or cause a denial of service (DOM tree corruption) via a web site with crafted JavaScript code and IFRAME elements.
CVE-2015-1292	The NavigatorServiceWorker::serviceWorker function in modules/serviceworkers/NavigatorServiceWorker.cpp in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy by accessing a Service Worker.
CVE-2015-1293	The DOM implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2015-1294	Use-after-free vulnerability in the SkMatrix::invertNonIdentity function in core/SkMatrix.cpp in Skia, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering the use of matrix elements that lead to an infinite result during an inversion calculation.
CVE-2015-1295	Multiple use-after-free vulnerabilities in the PrintWebViewHelper class in components/printing/renderer/print_web_view_helper.cc in Google Chrome before 45.0.2454.85 allow user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact by triggering nested IPC messages during preparation for printing, as demonstrated by messages associated with PDF documents in conjunction with messages about printer capabilities.
CVE-2015-1296	The UnescapeURLWithAdjustmentsImpl implementation in net/base/escape.cc in Google Chrome before 45.0.2454.85 does not prevent display of Unicode LOCK characters in the omnibox, which makes it easier for remote attackers to spoof the SSL lock icon by placing one of these characters at the end of a URL, as demonstrated by the omnibox in localizations for right-to-left languages.
CVE-2015-1297	The WebRequest API implementation in extensions/browser/api/web_request/web_request_api.cc in Google Chrome before 45.0.2454.85 does not properly consider a request's source before accepting the request, which allows remote attackers to bypass intended access restrictions via a crafted (1) app or (2) extension.
CVE-2015-1298	The RuntimeEventRouter::OnExtensionUninstalled function in extensions/browser/api/runtime/runtime_api.cc in Google Chrome before 45.0.2454.85 does not ensure that the setUninstallURL preference corresponds to the URL of a web site, which allows user-assisted remote attackers to trigger access to an arbitrary URL via a crafted extension that is uninstalled.
CVE-2015-1299	Use-after-free vulnerability in the shared-timer implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging erroneous timer firing, related to ThreadTimers.cpp and Timer.cpp.
CVE-2015-1300	The FrameFetchContext::updateTimingInfoForIFrameNavigation function in core/loader/FrameFetchContext.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to obtain sensitive information via crafted JavaScript code that leverages a history.back call.
CVE-2015-1301	Multiple unspecified vulnerabilities in Google Chrome before 45.0.2454.85 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1302	The PDF viewer in Google Chrome before 46.0.2490.86 does not properly restrict scripting messages and API exposure, which allows remote attackers to bypass the Same Origin Policy via an unintended embedder or unintended plugin loading, related to pdf.js and out_of_process_instance.cc.
CVE-2015-1303	bindings/core/v8/V8DOMWrapper.h in Blink, as used in Google Chrome before 45.0.2454.101, does not perform a rethrow action to propagate information about a cross-context exception, which allows remote attackers to bypass the Same Origin Policy via a crafted HTML document containing an IFRAME element.
CVE-2015-1304	object-observe.js in Google V8, as used in Google Chrome before 45.0.2454.101, does not properly restrict method calls on access-checked objects, which allows remote attackers to bypass the Same Origin Policy via a (1) observe or (2) getNotifier call.
CVE-2015-1346	Multiple unspecified vulnerabilities in Google V8 before 3.30.33.15, as used in Google Chrome before 40.0.2214.91, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1359	Multiple off-by-one errors in fpdfapi/fpdf_font/font_int.h in PDFium, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified

	other impact via a crafted PDF document, related to an "intra-object-overflow" issue, a different vulnerability than CVE-2015-1205.
CVE-2015-1360	Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted data that is improperly handled during text drawing, related to gpu/GrBitmapTextContext.cpp and gpu/GrDistanceFieldTextContext.cpp, a different vulnerability than CVE-2015-1205.
CVE-2015-1361	platform/image-decoders/ImageFrame.h in Blink, as used in Google Chrome before 40.0.2214.91, does not initialize a variable that is used in calls to the Skia SkBitmap::setAlphaType function, which might allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document, a different vulnerability than CVE-2015-1205.
CVE-2015-2238	Multiple unspecified vulnerabilities in Google V8 before 4.1.0.21, as used in Google Chrome before 41.0.2272.76, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-2239	Google Chrome before 41.0.2272.76, when Instant Extended mode is used, does not properly consider the interaction between the "1993 search" features and restore-from-disk RELOAD transitions, which makes it easier for remote attackers to spoof the address bar for a search-results page by leveraging (1) a compromised search engine or (2) an XSS vulnerability in a search engine, a different vulnerability than CVE-2015-1231.
CVE-2015-2808	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.
CVE-2015-3333	Multiple unspecified vulnerabilities in Google V8 before 4.2.77.14, as used in Google Chrome before 42.0.2311.90, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-3334	browser/ui/website_settings/website_settings.cc in Google Chrome before 42.0.2311.90 does not always display "Media: Allowed by you" in a Permissions table after the user has granted camera permission to a web site, which might make it easier for user-assisted remote attackers to obtain sensitive video data from a device's physical environment via a crafted web site that turns on the camera at a time when the user believes that camera access is prohibited.
CVE-2015-3335	The NaClSandbox::InitializeLayerTwoSandbox function in components/nacl/loader/sandbox_linux/nacl_sandbox_linux.cc in Google Chrome before 42.0.2311.90 does not have RLIMIT_AS and RLIMIT_DATA limits for Native Client (aka NaCl) processes, which might make it easier for remote attackers to conduct row-hammer attacks or have unspecified other impact by leveraging the ability to run a crafted program in the NaCl sandbox.
CVE-2015-3336	Google Chrome before 42.0.2311.90 does not always ask the user before proceeding with CONTENT_SETTINGS_TYPE_FULLSCREEN and CONTENT_SETTINGS_TYPE_MOUSELOCK changes, which allows user-assisted remote attackers to cause a denial of service (UI disruption) by constructing a crafted HTML document containing JavaScript code with requestFullScreen and requestPointerLock calls, and arranging for the user to access this document with a file: URL.
CVE-2015-3910	Multiple unspecified vulnerabilities in Google V8 before 4.3.61.21, as used in Google Chrome before 43.0.2357.65, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
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-2015-4491	Integer overflow in the make_filter_table function in pixops/pixops.c in gdk-pixbuf before 2.31.5, as used in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 on Linux, Google Chrome on Linux, and other products, allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and application crash) via crafted bitmap dimensions that are mishandled during scaling.
CVE-2015-5605	The regular-expression implementation in Google V8, as used in Google Chrome before 44.0.2403.89, mishandles interrupts, which allows remote attackers to cause a denial of service (application crash) via crafted JavaScript code, as demonstrated by an error in garbage collection during allocation of a stack-overflow exception message.
CVE-2015-6580	Multiple unspecified vulnerabilities in Google V8 before 4.5.103.29, as used in Google Chrome before 45.0.2454.85, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6581	Double free vulnerability in the opj_j2k_copy_default_tcp_and_create_tcd function in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 45.0.2454.85, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering a memory-allocation failure.
CVE-2015-6582	The decompose function in platform/transforms/TransformationMatrix.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not verify that a matrix inversion succeeded, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted web site.

CVE-2015-6583	Google Chrome before 45.0.2454.85 does not display a location bar for a hosted app's window after navigation away from the installation site, which might make it easier for remote attackers to spoof content via a crafted app, related to <code>browser.cc</code> and <code>hosted_app_browser_controller.cc</code> .
CVE-2015-6755	The ContainerNode::parserInsertBefore function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 46.0.2490.71, proceeds with a DOM tree insertion in certain cases where a parent node no longer contains a child node, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2015-6756	Use-after-free vulnerability in the CPDFSDK_PageView implementation in fpdfsdk/src/fsdk_mgr.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging mishandling of a focused annotation in a PDF document.
CVE-2015-6757	Use-after-free vulnerability in content/browser/service_worker/embedded_worker_instance.cc in the ServiceWorker implementation in Google Chrome before 46.0.2490.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging object destruction in a callback.
CVE-2015-6758	The CPDF_Document::GetPage function in fpdfapi/fpdf_parser/fpdf_parser_document.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, does not properly perform a cast of a dictionary object, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2015-6759	The shouldTreatAsUniqueOrigin function in platform/weborigin/SecurityOrigin.cpp in Blink, as used in Google Chrome before 46.0.2490.71, does not ensure that the origin of a LocalStorage resource is considered unique, which allows remote attackers to obtain sensitive information via vectors involving a blob: URL.
CVE-2015-6760	The Image11::map function in renderer/d3d/d3d11/Image11.cpp in libANGLE, as used in Google Chrome before 46.0.2490.71, mishandles mapping failures after device-lost events, which allows remote attackers to cause a denial of service (invalid read or write) or possibly have unspecified other impact via vectors involving a removed device.
CVE-2015-6761	The update_dimensions function in libavcodec/vp8.c in FFmpeg through 2.8.1, as used in Google Chrome before 46.0.2490.71 and other products, relies on a coefficient-partition count during multi-threaded operation, which allows remote attackers to cause a denial of service (race condition and memory corruption) or possibly have unspecified other impact via a crafted WebM file.
CVE-2015-6762	The CSSFontFaceSrcValue::fetch function in core/css/CSSFontFaceSrcValue.cpp in the Cascading Style Sheets (CSS) implementation in Blink, as used in Google Chrome before 46.0.2490.71, does not use the CORS cross-origin request algorithm when a font's URL appears to be a same-origin URL, which allows remote web servers to bypass the Same Origin Policy via a redirect.
CVE-2015-6763	Multiple unspecified vulnerabilities in Google Chrome before 46.0.2490.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6764	The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2015-6765	Use-after-free vulnerability in content/browser/appcache/appcache_update_job.cc in Google Chrome before 47.0.2526.73 allows remote attackers to execute arbitrary code or cause a denial of service by leveraging the mishandling of AppCache update jobs.
CVE-2015-6766	Use-after-free vulnerability in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers with renderer access to cause a denial of service or possibly have unspecified other impact by leveraging incorrect AppCacheUpdateJob behavior associated with duplicate cache selection.
CVE-2015-6767	Use-after-free vulnerability in content/browser/appcache/appcache_dispatcher_host.cc in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect pointer maintenance associated with certain callbacks.
CVE-2015-6768	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6770.
CVE-2015-6769	The provisional-load commit implementation in WebKit/Source/bindings/core/v8/WindowProxy.cpp in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy by leveraging a delay in window proxy clearing.
CVE-2015-6770	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6768.
CVE-2015-6771	js/array.js in Google V8, as used in Google Chrome before 47.0.2526.73, improperly implements certain map and filter operations for arrays, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2015-6772	The DOM implementation in Blink, as used in Google Chrome before 47.0.2526.73, does not prevent javascript: URL navigation while a document is being detached, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that improperly interacts with a plugin.

CVE-2015-6773	The convolution implementation in Skia, as used in Google Chrome before 47.0.2526.73, does not properly constrain row lengths, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted graphics data.
CVE-2015-6774	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that modifies a pointer used for reporting loadTimes data.
CVE-2015-6775	fpdfsdk/src/jsapi/fxjs_v8.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, does not use signatures, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-6776	The opj_dwt_decode_1* functions in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 47.0.2526.73, allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during a discrete wavelet transform.
CVE-2015-6777	Use-after-free vulnerability in the ContainerNode::notifyNodeInsertedInternal function in WebKit/Source/core/dom/ContainerNode.cpp in the DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOMCharacterDataModified events for certain detached-subtree insertions.
CVE-2015-6778	The CJBIG2_SymbolDict class in fxcodec/jbig2/JBig2_SymbolDict.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a PDF document containing crafted data with JBIG2 compression.
CVE-2015-6779	PDFium, as used in Google Chrome before 47.0.2526.73, does not properly restrict use of chrome: URLs, which allows remote attackers to bypass intended scheme restrictions via a crafted PDF document, as demonstrated by a document with a link to a chrome://settings URL.
CVE-2015-6780	Use-after-free vulnerability in the Infobars implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site, related to browser/ui/views/website_settings/website_settings_popup_view.cc.
CVE-2015-6781	Integer overflow in the FontData::Bound function in data/font_data.cc in Google sfntly, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted offset or length value within font data in an SFNT container.
CVE-2015-6782	The Document::open function in WebKit/Source/core/dom/Document.cpp in Google Chrome before 47.0.2526.73 does not ensure that page-dismissal event handling is compatible with modal-dialog blocking, which makes it easier for remote attackers to spoof Omnibox content via a crafted web site.
CVE-2015-6783	The FindStartOffsetOfFileInZipFile function in crazy_linker_zip.cpp in crazy_linker (aka Crazy Linker) in Android 5.x and 6.x, as used in Google Chrome before 47.0.2526.73, improperly searches for an EOCD record, which allows attackers to bypass a signature-validation requirement via a crafted ZIP archive.
CVE-2015-6784	The page serializer in Google Chrome before 47.0.2526.73 mishandles Mark of the Web (MOTW) comments for URLs containing a "--" sequence, which might allow remote attackers to inject HTML via a crafted URL, as demonstrated by an initial http://example.com?-- substring.
CVE-2015-6785	The CSPSource::hostMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts an x.y hostname as a match for a *.x.y pattern, which might allow remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging a policy that was intended to be specific to subdomains.
CVE-2015-6786	The CSPSourceList::matches function in WebKit/Source/core/frame/csp/CSPSourceList.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts a blob:, data:, or filesystem: URL as a match for a * pattern, which allows remote attackers to bypass intended scheme restrictions in opportunistic circumstances by leveraging a policy that relies on this pattern.
CVE-2015-6787	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.73 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6788	The ObjectBackedNativeHandler class in extensions/renderer/object_backed_native_handler.cc in the extensions subsystem in Google Chrome before 47.0.2526.80 improperly implements handler functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-6789	Race condition in the MutationObserver implementation in Blink, as used in Google Chrome before 47.0.2526.80, allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact by leveraging unanticipated object deletion.
CVE-2015-6790	The WebPageSerializerImpl::openTagToString function in WebKit/Source/web/WebPageSerializerImpl.cpp in the page serializer in Google Chrome before 47.0.2526.80 does not properly use HTML entities, which might allow remote attackers to inject arbitrary web script or HTML via a crafted document, as demonstrated by a double-quote character inside a single-quoted string.
CVE-2015-6791	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.80 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

CVE-2015-6792	The MIDI subsystem in Google Chrome before 47.0.2526.106 does not properly handle the sending of data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to midi_manager.cc, midi_manager_alsa.cc, and midi_manager_mac.cc, a different vulnerability than CVE-2015-8664.
CVE-2015-7834	Multiple unspecified vulnerabilities in Google V8 before 4.6.85.23, as used in Google Chrome before 46.0.2490.71, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-8478	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.73, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-8479	Use-after-free vulnerability in the AudioOutputDevice::OnDeviceAuthorized function in media/audio/audio_output_device.cc in Google Chrome before 47.0.2526.73 allows attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering access to an unauthorized audio output device.
CVE-2015-8480	The VideoFramePool::PoolImpl::CreateFrame function in media/base/video_frame_pool.cc in Google Chrome before 47.0.2526.73 does not initialize memory for a video-frame data structure, which might allow remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact by leveraging improper interaction with the vp3_h_loop_filter_c function in libavcodec/vp3dsp.c in FFmpeg.
CVE-2015-8548	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.80, allow attackers to cause a denial of service or possibly have other impact via unknown vectors, a different issue than CVE-2015-8478.
CVE-2015-8664	Integer overflow in the WebCursor::Deserialize function in content/common/cursors/webcursor.cc in Google Chrome before 47.0.2526.106 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an RGBA pixel array with crafted dimensions, a different vulnerability than CVE-2015-6792.
CVE-2016-1612	The LoadIC::UpdateCaches function in ic/ic.cc in Google V8, as used in Google Chrome before 48.0.2564.82, does not ensure receiver compatibility before performing a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact via crafted JavaScript code.
CVE-2016-1613	Multiple use-after-free vulnerabilities in the formfiller implementation in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to improper tracking of the destruction of (1) IPWL_FocusHandler and (2) IPWL_Provider objects.
CVE-2016-1614	The UnacceleratedImageBufferSurface class in WebKit/Source/platform/graphics/UnacceleratedImageBufferSurface.cpp in Blink, as used in Google Chrome before 48.0.2564.82, mishandles the initialization mode, which allows remote attackers to obtain sensitive information from process memory via a crafted web site.
CVE-2016-1615	The Omnibox implementation in Google Chrome before 48.0.2564.82 allows remote attackers to spoof a document's origin via unspecified vectors.
CVE-2016-1616	The CustomButton::AcceleratorPressed function in ui/views/controls/button/custom_button.cc in Google Chrome before 48.0.2564.82 allows remote attackers to spoof URLs via vectors involving an unfocused custom button.
CVE-2016-1617	The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 48.0.2564.82, does not apply http policies to https URLs and does not apply ws policies to wss URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report.
CVE-2016-1618	Blink, as used in Google Chrome before 48.0.2564.82, does not ensure that a proper cryptographicallyRandomValues random number generator is used, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.
CVE-2016-1619	Multiple integer overflows in the (1) sycc422_to_rgb and (2) sycc444_to_rgb functions in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted PDF document.
CVE-2016-1620	Multiple unspecified vulnerabilities in Google Chrome before 48.0.2564.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1622	The Extensions subsystem in Google Chrome before 48.0.2564.109 does not prevent use of the Object.defineProperty method to override intended extension behavior, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-1623	The DOM implementation in Google Chrome before 48.0.2564.109 does not properly restrict frame-attach operations from occurring during or after frame-detach operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, related to FrameLoader.cpp, HTMLFrameOwnerElement.h, LocalFrame.cpp, and WebLocalFrameImpl.cpp.
CVE-2016-1624	Integer underflow in the ProcessCommandsInternal function in dec/decode.c in Brotli, as used in Google Chrome before 48.0.2564.109, allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted data with brotli compression.

CVE-2016-1625	The Chrome Instant feature in Google Chrome before 48.0.2564.109 does not ensure that a New Tab Page (NTP) navigation target is on the most-visited or suggestions list, which allows remote attackers to bypass intended restrictions via unspecified vectors, related to instant_service.cc and search_tab_helper.cc.
CVE-2016-1626	The opj_pi_update_decode_poc function in pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, miscalculates a certain layer index value, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2016-1627	The Developer Tools (aka DevTools) subsystem in Google Chrome before 48.0.2564.109 does not validate URL schemes and ensure that the remoteBase parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote attackers to bypass intended access restrictions via a crafted URL, related to browser/devtools/devtools_ui_bindings.cc and WebKit/Source/devtools/front_end/Runtime.js.
CVE-2016-1628	pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, does not validate a certain precision value, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via a crafted JPEG 2000 image in a PDF document, related to the opj_pi_next_rpcl, opj_pi_next_pcrl, and opj_pi_next_cprl functions.
CVE-2016-1629	Google Chrome before 48.0.2564.116 allows remote attackers to bypass the Blink Same Origin Policy and a sandbox protection mechanism via unspecified vectors.
CVE-2016-1630	The ContainerNode::parserRemoveChild function in WebKit/Source/core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 49.0.2623.75, mishandles widget updates, which makes it easier for remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1631	The PPB_Flash_MessageLoop_Impl::InternalRun function in content/renderer/pepper/ppb_flash_message_loop_impl.cc in the Pepper plugin in Google Chrome before 49.0.2623.75 mishandles nested message loops, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1632	The Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly maintain own properties, which allows remote attackers to bypass intended access restrictions via crafted JavaScript code that triggers an incorrect cast, related to extensions/renderer/v8_helpers.h and gin/converter.h.
CVE-2016-1633	Use-after-free vulnerability in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1634	Use-after-free vulnerability in the StyleResolver::appendCSSStyleSheet function in WebKit/Source/core/css/resolver/StyleResolver.cpp in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that triggers Cascading Style Sheets (CSS) style invalidation during a certain subtree-removal action.
CVE-2016-1635	extensions/renderer/render_frame_observer_natives.cc in Google Chrome before 49.0.2623.75 does not properly consider object lifetimes and re-entrancy issues during OnDocumentElementCreated handling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1636	The PendingScript::notifyFinished function in WebKit/Source/core/dom/PendingScript.cpp in Google Chrome before 49.0.2623.75 relies on memory-cache information about integrity-check occurrences instead of integrity-check successes, which allows remote attackers to bypass the Subresource Integrity (aka SRI) protection mechanism by triggering two loads of the same resource.
CVE-2016-1637	The SkATan2_255 function in effects/gradients/SkSweepGradient.cpp in Skia, as used in Google Chrome before 49.0.2623.75, mishandles arctangent calculations, which allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2016-1638	extensions/renderer/resources/platform_app.js in the Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly restrict use of Web APIs, which allows remote attackers to bypass intended access restrictions via a crafted platform app.
CVE-2016-1639	Use-after-free vulnerability in browser/extensions/api/webrtc_audio_private/webrtc_audio_private_api.cc in the WebRTC Audio Private API implementation in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect reliance on the resource context pointer.
CVE-2016-1640	The Web Store inline-installer implementation in the Extensions UI in Google Chrome before 49.0.2623.75 does not block installations upon deletion of an installation frame, which makes it easier for remote attackers to trick a user into believing that an installation request originated from the user's next navigation target via a crafted web site.
CVE-2016-1641	Use-after-free vulnerability in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an image download after a certain data structure is deleted, as demonstrated by a favicon.ico download.
CVE-2016-1642	Multiple unspecified vulnerabilities in Google Chrome before 49.0.2623.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1643	The ImageInputType::ensurePrimaryContent function in WebKit/Source/core/html/forms/ImageInputType.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly maintain the user agent shadow DOM,

	which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2016-1644	WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict relayout scheduling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted HTML document.
CVE-2016-1645	Multiple integer signedness errors in the opj_j2k_update_image_data function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 49.0.2623.87, allow remote attackers to cause a denial of service (incorrect cast and out-of-bounds write) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-1646	The Array.prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1647	Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/browser/renderer_host/render_widget_host_impl.cc in the Navigation implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1648	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1649	The Program::getUniformInternal function in Program.cpp in libANGLE, as used in Google Chrome before 49.0.2623.108, does not properly handle a certain data-type mismatch, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted shader stages.
CVE-2016-1650	The PageCaptureSaveAsMHTMLFunction::ReturnFailure function in browser/extensions/api/page_capture/page_capture_api.cc in Google Chrome before 49.0.2623.108 allows attackers to cause a denial of service or possibly have unspecified other impact by triggering an error in creating an MHTML document.
CVE-2016-2051	Multiple unspecified vulnerabilities in Google V8 before 4.8.271.17, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-2052	Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via crafted data, as demonstrated by a buffer over-read resulting from an inverted length check in hb-ot-font.cc, a different issue than CVE-2015-8947.
CVE-2016-2843	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.26, as used in Google Chrome before 49.0.2623.75, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-2844	WebKit/Source/core/layout/LayoutBlock.cpp in Blink, as used in Google Chrome before 49.0.2623.75, does not properly determine when anonymous block wrappers may exist, which allows remote attackers to cause a denial of service (incorrect cast and assertion failure) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-2845	The Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 49.0.2623.75, does not ignore a URL's path component in the case of a ServiceWorker fetch, which allows remote attackers to obtain sensitive information about visited web pages by reading CSP violation reports, related to FrameFetchContext.cpp and ResourceFetcher.cpp.
CVE-2016-3679	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.33, as used in Google Chrome before 49.0.2623.108, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

## Firefox CVEs

cve_id	description
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-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-2010-2179	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, when Firefox or Chrome is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to URL parsing.
CVE-2011-1300	The Program::getActiveUniformMaxLength function in libGLESv2/Program.cpp in libGLESv2.dll in the WebGLES library in Almost Native Graphics Layer Engine (ANGLE), as used in Mozilla Firefox 4.x before 4.0.1

	on Windows and in the GPU process in Google Chrome before 10.0.648.205 on Windows, allows remote attackers to execute arbitrary code via unspecified vectors, related to an "off-by-three" error.
CVE-2011-3389	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
CVE-2012-4929	The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.
CVE-2012-4930	The SPDY protocol 3 and earlier, as used in Mozilla Firefox, Google Chrome, and other products, can perform TLS encryption of compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.
CVE-2013-1489	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 10 and Update 11, when running on Windows using Internet Explorer, Firefox, Opera, and Google Chrome, allows remote attackers to bypass the "Very High" security level of the Java Control Panel and execute unsigned Java code without prompting the user via unknown vectors, aka "Issue 53" and the "Java Security Slider" vulnerability.
CVE-2013-2566	The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.
CVE-2015-2808	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.
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-2015-4491	Integer overflow in the make_filter_table function in pixops/pixops.c in gdk-pixbuf before 2.31.5, as used in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 on Linux, Google Chrome on Linux, and other products, allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and application crash) via crafted bitmap dimensions that are mishandled during scaling.
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-2002-2437	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 sensitive information about visited web pages by calling this method.
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-2004-0757	Heap-based buffer overflow in the SendUidl in the POP3 capability for Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, may allow remote POP3 mail servers to execute arbitrary code.
CVE-2004-0761	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote attackers to use certain redirect sequences to spoof the security lock icon that makes a web page appear to be encrypted.
CVE-2004-0762	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to install arbitrary extensions by using interactive events to manipulate the XPIInstall Security dialog box.
CVE-2004-0764	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to hijack the user interface via the "chrome" flag and XML User Interface Language (XUL) files.
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-2004-0904	Integer overflow in the bitmap (BMP) decoder for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to execute arbitrary code via wide bitmap files that trigger heap-based buffer overflows.
CVE-2005-0142	Firefox 0.9, Thunderbird 0.6 and other versions before 0.9, and Mozilla 1.7 before 1.7.5 save temporary files with world-readable permissions, which allows local users to read certain web content or attachments that belong to other users, e.g. content that is managed by helper applications such as PDF.

CVE-2005-0255	String handling functions in Mozilla 1.7.3, Firefox 1.0, and Thunderbird before 1.0.2, such as the nsTSubstring_CharT::Replace function, do not properly check the return values of other functions that resize the string, which allows remote attackers to cause a denial of service and possibly execute arbitrary code by forcing an out-of-memory state that causes a reallocation to fail and return a pointer to a fixed address, which leads to heap corruption.
CVE-2005-0399	Heap-based buffer overflow in GIF2.cpp in Firefox before 1.0.2, Mozilla before 1.7.6, and Thunderbird before 1.0.2, and possibly other applications that use the same library, allows remote attackers to execute arbitrary code via a GIF image with a crafted Netscape extension 2 block and buffer size.
CVE-2005-0590	The installation confirmation dialog in Firefox before 1.0.1, Thunderbird before 1.0.1, and Mozilla before 1.7.6 allows remote attackers to use InstallTrigger to spoof the hostname of the host performing the installation via a long "user:pass" sequence in the URL, which appears before the real hostname.
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-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-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-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-2006-0295	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 QueryInterface method of the built-in Location and Navigator objects, which leads to memory corruption.
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) nsSVG CairoSurface::Init in SVG, and (3) nsCanvasRenderingContext2D.cpp in Canvas.
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-2006-0748	Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to execute arbitrary code via "an invalid and non-sensical ordering of table-related tags" that results in a negative array index.
CVE-2006-0749	nsHTMLContentSink.cpp 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) and possibly execute arbitrary code via unknown vectors involving a "particular sequence of HTML tags" that leads to memory corruption.
CVE-2006-1529	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1530	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1531	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1723	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1724	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via attack vectors related to DHTML.
CVE-2006-1725	Mozilla Firefox 1.5 before 1.5.0.2 and SeaMonkey before 1.0.1 causes certain windows to become translucent due to an interaction between XUL content windows and the history mechanism, which might allow user-assisted remote attackers to trick users into executing arbitrary code.

CVE-2006-1726	Unspecified vulnerability in Firefox and Thunderbird 1.5 before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to bypass the js_ValueToFunctionObject check and execute arbitrary code via unknown vectors involving setTimeout and Firefox' ForEach method.
CVE-2006-1727	Unspecified vulnerability in Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to gain chrome privileges via multiple attack vectors related to the use of XBL scripts with "Print Preview".
CVE-2006-1728	Unspecified vulnerability in Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to execute arbitrary code via unknown vectors related to the crypto.generateCRMFRequest method.
CVE-2006-1729	Mozilla Firefox 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to read arbitrary files by (1) inserting the target filename into a text box, then turning that box into a file upload control, or (2) changing the type of the input control that is associated with an event handler.
CVE-2006-1730	Integer overflow in Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to execute arbitrary code via a large number in the CSS letter-spacing property that leads to a heap-based buffer overflow.
CVE-2006-1731	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 returns the Object class prototype instead of the global window object when (1) .valueOf.call or (2) .valueOf.apply are called without any arguments, which allows remote attackers to conduct cross-site scripting (XSS) attacks.
CVE-2006-1732	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 bypass same-origin protections and conduct cross-site scripting (XSS) attacks via unspecified vectors involving the window.controllers array.
CVE-2006-1733	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 does not properly protect the compilation scope of privileged built-in XBL bindings, which allows remote attackers to execute arbitrary code via the (1) valueOf.call or (2) valueOf.apply methods of an XBL binding, or (3) "by inserting an XBL method into the DOM's document.body prototype chain."
CVE-2006-1734	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 execute arbitrary code by using the Object.watch method to access the "clone parent" internal function.
CVE-2006-1735	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 execute arbitrary code by using an eval in an XBL method binding (XBL.method.eval) to create Javascript functions that are compiled with extra privileges.
CVE-2006-1736	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 trick users into downloading and saving an executable file via an image that is overlaid by a transparent image link that points to the executable, which causes the executable to be saved when the user clicks the "Save image as..." option. NOTE: this attack is made easier due to a GUI truncation issue that prevents the user from seeing the malicious extension when there is extra whitespace in the filename.
CVE-2006-1737	Integer overflow 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) and possibly execute arbitrary bytecode via JavaScript with a large regular expression.
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-2006-1739	The CSS border-rendering code 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) and possibly execute arbitrary code via certain Cascading Style Sheets (CSS) that causes an out-of-bounds array write and buffer overflow.
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-2006-1741	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 inject arbitrary Javascript into other sites by (1) "using a modal alert to suspend an event handler while a new page is being loaded", (2) using eval(), and using certain variants involving (3) "new Script;" and (4) using window.__proto__ to extend eval, aka "cross-site JavaScript injection".
CVE-2006-1742	The JavaScript engine 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 does not properly handle temporary variables that are not garbage collected, which might allow remote attackers to trigger operations on freed memory and cause memory corruption.
CVE-2006-2775	Mozilla Firefox and Thunderbird before 1.5.0.4 associates XUL attributes with the wrong URL under certain unspecified circumstances, which might allow remote attackers to bypass restrictions by causing a persisted string to be associated with the wrong URL.

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-2006-2778	The crypto.signText function in Mozilla Firefox and Thunderbird before 1.5.0.4 allows remote attackers to execute arbitrary code via certain optional Certificate Authority name arguments, which causes an invalid array index and triggers a buffer overflow.
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-2006-2780	Integer overflow in Mozilla Firefox and Thunderbird before 1.5.0.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via "jsstr tagify," which leads to memory corruption.
CVE-2006-2783	Mozilla Firefox and Thunderbird before 1.5.0.4 strip the Unicode Byte-order-Mark (BOM) from a UTF-8 page before the page is passed to the parser, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a BOM sequence in the middle of a dangerous tag such as SCRIPT.
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-2006-2787	EvalInSandbox in Mozilla Firefox and Thunderbird before 1.5.0.4 allows remote attackers to gain privileges via javascript that calls the valueOf method on objects that were created outside of the sandbox.
CVE-2006-3113	Mozilla Firefox 1.5 before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via simultaneous XPCOM events, which causes a timer object to be deleted in a way that triggers memory corruption.
CVE-2006-3802	Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to hijack native DOM methods from objects in another domain and conduct cross-site scripting (XSS) attacks using DOM methods of the top-level object.
CVE-2006-3803	Race condition in the JavaScript garbage collection in Mozilla Firefox 1.5 before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 might allow remote attackers to execute arbitrary code by causing the garbage collector to delete a temporary variable while it is still being used during the creation of a new Function object.
CVE-2006-3805	The Javascript engine in Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 might allow remote attackers to execute arbitrary code via vectors involving garbage collection that causes deletion of a temporary object that is still being used.
CVE-2006-3806	Multiple integer overflows in the Javascript engine in Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 might allow remote attackers to execute arbitrary code via vectors involving (1) long strings in the toSource method of the Object, Array, and String objects; and (2) unspecified "string function arguments."
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-2006-3809	Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows scripts with the UniversalBrowserRead privilege to gain UniversalXPConnect privileges and possibly execute code or obtain sensitive data by reading into a privileged context.
CVE-2006-3810	Cross-site scripting (XSS) vulnerability in Mozilla Firefox 1.5 before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to inject arbitrary web script or HTML via the XPCNativeWrapper(window).Function construct.
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-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-2006-4340	Mozilla Network Security Service (NSS) library before 3.11.3, as used in Mozilla Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5, when using an RSA key with exponent 3, does not properly handle extra data in a signature, which allows remote attackers to forge signatures for SSL/TLS and email certificates, a similar vulnerability to CVE-2006-4339. NOTE: on 20061107, Mozilla released an advisory stating that these versions were not completely patched by MFSA2006-60. The newer fixes for 1.5.0.7 are covered by CVE-2006-5462.

CVE-2006-4565	Heap-based buffer overflow in Mozilla Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a JavaScript regular expression with a "minimal quantifier."
CVE-2006-4566	Mozilla Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5 allows remote attackers to cause a denial of service (crash) via a malformed JavaScript regular expression that ends with a backslash in an unterminated character set ("\\\"), which leads to a buffer over-read.
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-2006-5462	Mozilla Network Security Service (NSS) library before 3.11.3, as used in Mozilla Firefox before 1.5.0.8, Thunderbird before 1.5.0.8, and SeaMonkey before 1.0.6, when using an RSA key with exponent 3, does not properly handle extra data in a signature, which allows remote attackers to forge signatures for SSL/TLS and email certificates. NOTE: this identifier is for unpatched product versions that were originally intended to be addressed by CVE-2006-4340.
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-2006-5464	Multiple unspecified vulnerabilities in the layout 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) via unspecified vectors.
CVE-2006-5747	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 code via the XML.prototype.hasOwnProperty JavaScript function.
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-2006-6497	Multiple unspecified vulnerabilities in the layout engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown attack vectors.
CVE-2006-6498	Multiple unspecified vulnerabilities in the JavaScript engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, SeaMonkey before 1.0.7, and Mozilla 1.7 and probably earlier on Solaris, allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown impact and attack vectors.
CVE-2006-6499	The js_dtoa function in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 overwrites memory instead of exiting when the floating point precision is reduced, which allows remote attackers to cause a denial of service via any plugins that reduce the precision.
CVE-2006-6500	Heap-based buffer overflow in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by setting the CSS cursor to certain images that cause an incorrect size calculation when converting to a Windows bitmap.
CVE-2006-6501	Unspecified vulnerability in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to gain privileges and install malicious code via the watch Javascript function.
CVE-2006-6502	Use-after-free vulnerability in the LiveConnect bridge code for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to cause a denial of service (crash) via unknown vectors.
CVE-2006-6503	Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to bypass cross-site scripting (XSS) protection by changing the src attribute of an IMG element to a javascript: URI.
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-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-2007-0009	Stack-based buffer overflow 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, Thunderbird before 1.5.0.10, SeaMonkey before 1.0.8, and

	certain Sun Java System server products before 20070611, allows remote attackers to execute arbitrary code via invalid "Client Master Key" length values.
CVE-2007-0775	Multiple unspecified vulnerabilities in the layout 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 allow remote attackers to cause a denial of service (crash) and potentially execute arbitrary code via certain vectors.
CVE-2007-0776	Heap-based buffer overflow in the _cairo_pen_init function in Mozilla Firefox 2.x before 2.0.0.2, Thunderbird before 1.5.0.10, and SeaMonkey before 1.0.8 allows remote attackers to execute arbitrary code via a large stroke-width attribute in the clipPath element in an SVG file.
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-2007-2867	Multiple vulnerabilities in the layout 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) via vectors related to dangling pointers, heap corruption, signed/unsigned, and other issues.
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-2007-3734	Multiple unspecified vulnerabilities in the browser 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-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-2007-3844	Mozilla Firefox 2.0.0.5, Thunderbird 2.0.0.5 and before 1.5.0.13, and SeaMonkey 1.1.3 allows remote attackers to conduct cross-site scripting (XSS) attacks with chrome privileges via an addon that inserts a (1) javascript: or (2) data: link into an about:blank document loaded by chrome via (a) the window.open function or (b) a content.location assignment, aka "Cross Context Scripting." NOTE: this issue is caused by a CVE-2007-3089 regression.
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-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-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-2007-5339	Multiple vulnerabilities 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 or assert errors.
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-2008-0412	The browser engine in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via vectors related to the (1) nsTableFrame::GetFrameAtOrBefore, (2) nsAccessibilityService::GetAccessible, (3) nsBindingManager::GetNestedInsertionPoint, (4) nsXBLPrototypeBinding::AttributeChanged, (5) nsColumnSetFrame::GetContentInsertionFrame, and (6) nsLineLayout::TrimTrailingWhiteSpaceIn methods, and other vectors.
CVE-2008-0413	The JavaScript engine in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via (1) a large switch statement, (2) certain uses of watch and eval, (3) certain uses of the mousedown event listener, and other vectors.
CVE-2008-0415	Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allows remote attackers to execute script outside of the sandbox and conduct cross-site scripting (XSS) attacks via multiple vectors including the XMLHttpRequest.load function, aka "JavaScript privilege escalation bugs."

CVE-2008-0416	Multiple cross-site scripting (XSS) vulnerabilities in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allow remote attackers to inject arbitrary web script or HTML via certain character encodings, including (1) a backspace character that is treated as whitespace, (2) 0x80 with Shift_JIS encoding, and (3) "zero-length non-ASCII sequences" in certain Asian character sets.
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-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-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-2008-1233	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 "XPCNativeWrapper pollution."
CVE-2008-1234	Cross-site scripting (XSS) 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 inject arbitrary web script or HTML via event handlers, aka "Universal XSS using event handlers."
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-2008-1236	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors related to the layout engine.
CVE-2008-1237	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors related to the JavaScript engine.
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-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-2008-2798	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via unknown vectors related to the layout engine.
CVE-2008-2799	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via unknown vectors related to the JavaScript engine.
CVE-2008-2802	Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 allow remote attackers to execute arbitrary code via an XUL document that includes a script from a chrome: URI that points to a fastload file, related to this file's "privilege level."
CVE-2008-2803	The mozIJSSubScriptLoader.LoadScript function in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 does not apply XPCNativeWrappers to scripts loaded from (1) file: URIs, (2) data: URIs, or (3) certain non-canonical chrome: URIs, which allows remote attackers to execute arbitrary code via vectors involving third-party add-ons.
CVE-2008-2806	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 on Mac OS X allow remote attackers to bypass the Same Origin Policy and create arbitrary socket connections via a crafted Java applet, related to the Java Embedding Plugin (JEP) and Java LiveConnect.
CVE-2008-2808	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 do not properly escape HTML in file:// URLs in directory listings, which allows remote attackers to conduct cross-site scripting (XSS) attacks or have unspecified other impact via a crafted filename.
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-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-2008-4058	The XPCConnect 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-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-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-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-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-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-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-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-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-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-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-2008-5018	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-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-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-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-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-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-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-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 GetXMLElement and FastAppendChar functions.
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-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-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-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-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-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-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-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-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-2009-0652	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-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-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-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-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-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-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-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-2009-1302	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-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 nsSVGEElement::BindToTree.
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-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 JSOPROP_PERMANENT attribute.
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-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-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-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-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) nsEventManager::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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2009-3983	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2010-1199	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.
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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2010-2769	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 added to a document in which the designMode property is enabled.
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-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-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-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-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-2010-3169	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-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-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-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-2010-3175	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-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-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-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-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-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-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-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-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-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-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-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-2010-3777	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-2010-3778	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-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-2011-0053	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-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-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-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-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-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-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-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-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-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-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-2011-0080	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2011-2377	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-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-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-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-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-2011-2982	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-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-2011-2984	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2011-3647	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-2011-3648	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-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-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-2011-3651	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 7.0 and Thunderbird 7.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
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-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-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-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-2011-3658	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 unspecified other impact via vectors involving removal of SVG elements.
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-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-2011-3661	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-2011-3663	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-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-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-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-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-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-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-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-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-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-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-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-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-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-2012-0451	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-2012-0452	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-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-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-2012-0456	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-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-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-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-2012-0460	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-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-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-2012-0463	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-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-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-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-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-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-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-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-2012-0473	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-2012-0474	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-2012-0475	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-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-2012-0478	The texImage2D implementation in the WebGL subsystem 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 does not properly restrict JSVAL_TO_OBJECT casts, which might allow remote attackers to execute arbitrary code via a crafted web page.
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-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.
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-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-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-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-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-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-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-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-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-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-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-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-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-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-2012-1954	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-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-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-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-2012-1958	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-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-2012-1960	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-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-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-2012-1963	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 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-2012-1964	The certificate-warning functionality in browser/components/certerror/content/aboutCertError.xhtml in Mozilla Firefox 4.x through 12.0, 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-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-2012-1970	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-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-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-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-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-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-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-2012-3105	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-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-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-2012-3958	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-2012-3959	Use-after-free vulnerability in the nsRangeUpdater::SelAdjDeleteNode 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-2012-3960	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-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-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-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-2012-3964	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-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-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-2012-3968	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-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-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-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-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-2012-3974	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-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-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-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-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-2012-3982	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-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-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-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-2012-3986	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-2012-3988	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-2012-3989	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-2012-3990	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-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-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-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-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-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-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-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-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-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-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-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-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-2012-4186	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-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-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-2012-4191	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-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-2012-4193	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-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-2012-4195	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-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-2012-4201	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-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-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-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-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-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-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-2012-4212	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-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-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-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-2012-4216	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-2012-4217	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-2012-4218	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-2012-5354	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-2012-5829	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2013-0754	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-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-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-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 <code>Object.prototype.__proto__</code> in a crafted HTML document.
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-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-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-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-2013-0762	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-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-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-2013-0765	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-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-2013-0767	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-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-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-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-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-2013-0772	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-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-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-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-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-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-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-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-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-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-2013-0782	Heap-based buffer overflow in the nsSaveAsCharset::DoCharsetConversion 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 unspecified vectors.
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-2013-0784	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-2013-0787	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-2013-0788	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-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-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-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-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-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-2013-0799	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-2013-0800	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-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-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-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-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-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-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-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-2013-1678	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 operation) via unspecified 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-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-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-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-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-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-2013-1686	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-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-2013-1690	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-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-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-2013-1694	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-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-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-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-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-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-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-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-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-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-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-2013-1718	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-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-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-2013-1722	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-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-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-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-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-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-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-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-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-2013-1736	The nsGfxScrollViewInner::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-2013-1737	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-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-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-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-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-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-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-2013-5597	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-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-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-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-2013-5602	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-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-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-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-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-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-2013-5616	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-2013-5618	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-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-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-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-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-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-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-2014-1486	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-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-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-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-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-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-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-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-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-2014-1509	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 that renders fonts in a PDF document.
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-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-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-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-2014-1514	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 code or cause a denial of service (out-of-bounds write and application crash) by triggering incorrect use of the TypedArrayObject class.
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-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-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-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-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-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-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-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-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-2014-1541	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 service (heap memory corruption) via crafted web content.
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-2014-1547	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2014-1567	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-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-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-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-2014-1578	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-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-2014-1585	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-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-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-2014-1590	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-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-2014-1593	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-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-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-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-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-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-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-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-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-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-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-2015-0816	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 Same Origin Policy, as demonstrated by the resource: URL associated with PDF.js.
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-2015-0827	Heap-based buffer overflow in the mozilla::gfx::CopyRect function in Mozilla Firefox before 36.0, Firefox ESR 31.x before 31.5, and Thunderbird before 31.5 allows remote attackers to obtain sensitive information from uninitialized process memory via a malformed SVG graphic.

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-2015-0833	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 DLL in (1) the current working directory or (2) a temporary directory, as demonstrated by bcrypt.dll.
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-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-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-2015-2713	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-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-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-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-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-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-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-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-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-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-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-2015-2738	The YCbCrImageDeserializer::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-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-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-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-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-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-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-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-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-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-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-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-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-2003-1492	Netscape Navigator 7.0.2 and Mozilla allows remote attackers to access cookie information in a different domain via an HTTP request for a domain with an extra .(dot) at the end.
CVE-2004-0763	Mozilla Firefox 0.9.1 and 0.9.2 allows remote web sites to spoof certificates of trusted web sites via redirects and Javascript that uses the "onunload" method.
CVE-2004-0779	The (1) Mozilla 1.6, (2) Firebird 0.7 and (3) Firefox 0.8 web browsers do not properly verify that cached passwords for SSL encrypted sites are only sent via SSL encrypted sessions to the site, which allows a remote attacker to cause a cached password to be sent in cleartext to a spoofed site.
CVE-2004-0866	Internet Explorer 6.0 allows web sites to set cookies for country-specific top-level domains, such as .ltd.uk, .plc.uk, and .sch.uk, which could allow remote attackers to perform a session fixation attack and hijack a user's HTTP session.
CVE-2004-0867	Mozilla Firefox 0.9.2 allows web sites to set cookies for country-specific top-level domains, such as .ltd.uk, .plc.uk, and .sch.uk, which could allow remote attackers to perform a session fixation attack and hijack a user's HTTP session. NOTE: it was later reported that 2.x is also affected.
CVE-2004-0905	Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows remote attackers to perform cross-domain scripting and possibly execute arbitrary code by convincing a user to drag and drop javascript: links to a frame or page in another domain.
CVE-2004-1156	Mozilla before 1.7.6, and Firefox before 1.0.1, allows remote attackers to spoof arbitrary web sites by injecting content from one window into a target window whose name is known but resides in a different domain, as demonstrated using a pop-up window on a trusted web site, aka the "window injection" vulnerability.
CVE-2004-1200	Firefox and Mozilla allow remote attackers to cause a denial of service (application crash from memory consumption), as demonstrated using Javascript code that continuously creates nested arrays and then sorts the newly created arrays.
CVE-2004-1380	Firefox before 1.0 and Mozilla before 1.7.5 allows inactive (background) tabs to launch dialog boxes, which can allow remote attackers to spoof the dialog boxes from web sites in other windows and facilitate phishing attacks, aka the "Dialog Box Spoofing Vulnerability."

CVE-2004-1381	Firefox before 1.0 and Mozilla before 1.7.5 allow inactive (background) tabs to focus on input being entered in the active tab, as originally reported using form fields, which allows remote attackers to steal sensitive data that is intended for other sites, which could facilitate phishing attacks.
CVE-2004-1639	Mozilla Firefox before 0.10, Mozilla 5.0, and Gecko 20040913 allows remote attackers to cause a denial of service (application crash or memory consumption) via a large binary file with a .html extension.
CVE-2004-1753	The Apple Java plugin, as used in Netscape 7.1 and 7.2, Mozilla 1.7.2, and Firefox 0.9.3 on Mac OS X 10.3.5, when tabbed browsing is enabled, does not properly handle SetWindow(NULL) calls, which allows Java applets from one tab to draw to other tabs and facilitates phishing attacks that spoof tabs.
CVE-2004-2225	Mozilla Firefox before 0.10.1 allows remote attackers to delete arbitrary files in the download directory via a crafted data: URI that is not properly handled when the user clicks the Save button.
CVE-2004-2227	Mozilla Firefox before 1.0 truncates long filenames in the file download dialog box, which makes it easier for remote attackers to trick users into downloading files with dangerous extensions.
CVE-2004-2228	Mozilla Firefox before 1.0 is installed with world-writable permissions on Mac OS X, which allows local users to gain privileges.
CVE-2004-2657	** DISPUTED ** Mozilla Firefox 1.5.0.1, and possibly other versions, preserves some records of user activity even after uninstalling, which allows local users who share a Windows profile to view the records after a new installation of Firefox, as reported for the list of Passwords Never Saved web sites. NOTE: The vendor has disputed this issue, stating that "The uninstaller is primarily there to uninstall the application. It is not there to uninstall user data. For the moment I will stick by my module-owner decision."
CVE-2005-0141	Firefox before 1.0 and Mozilla before 1.7.5 allow remote attackers to load local files via links "with a custom getter and toString method" that are middle-clicked by the user to be opened in a new tab.
CVE-2005-0143	Firefox before 1.0 and Mozilla before 1.7.5 display the SSL lock icon when an insecure page loads a binary file from a trusted site, which could facilitate phishing attacks.
CVE-2005-0144	Firefox before 1.0 and Mozilla before 1.7.5 display the secure site lock icon when a view-source: URL references a secure SSL site while an insecure page is being loaded, which could facilitate phishing attacks.
CVE-2005-0145	Firefox before 1.0 does not properly distinguish between user-generated and synthetic click events, which allows remote attackers to use Javascript to bypass the file download prompt when the user uses the Alt-click feature.
CVE-2005-0146	Firefox before 1.0 and Mozilla before 1.7.5 allow remote attackers to obtain sensitive data from the clipboard via Javascript that generates a middle-click event on systems for which a middle-click performs a paste operation.
CVE-2005-0147	Firefox before 1.0 and Mozilla before 1.7.5, when configured to use a proxy, respond to 407 proxy auth requests from arbitrary servers, which allows remote attackers to steal NTLM or SPNEGO credentials.
CVE-2005-0150	Firefox before 1.0 allows the user to store a (1) javascript: or (2) data: URLs as a Livefeed bookmark, then executes it in the security context of the currently loaded page when the user later accesses the bookmark, which could allow remote attackers to execute arbitrary code.
CVE-2005-0230	Firefox 1.0 does not prevent the user from dragging an executable file to the desktop when it has an image/gif content type but has a dangerous extension such as .bat or .exe, which allows remote attackers to bypass the intended restriction and execute arbitrary commands via malformed GIF files that can still be parsed by the Windows batch file parser, aka "firedragging."
CVE-2005-0231	Firefox 1.0 does not invoke the Javascript Security Manager when a user drags a javascript: or data: URL to a tab, which allows remote attackers to bypass the security model, aka "firetabbing."
CVE-2005-0232	Firefox 1.0 allows remote attackers to modify Boolean configuration parameters for the about:config site by using a plugin such as Flash, and the -moz-opacity filter, to display the about:config site then cause the user to double-click at a certain screen position, aka "Fireflashing."
CVE-2005-0233	The International Domain Name (IDN) support in Firefox 1.0, Camino 8.5, and Mozilla before 1.7.6 allows remote attackers to spoof domain names using punycode encoded domain names that are decoded in URLs and SSL certificates in a way that uses homograph characters from other character sets, which facilitates phishing attacks.
CVE-2005-0238	The International Domain Name (IDN) support in Epiphany allows remote attackers to spoof domain names using punycode encoded domain names that are decoded in URLs and SSL certificates in a way that uses homograph characters from other character sets, which facilitates phishing attacks.
CVE-2005-0401	FireFox 1.0.1 and Mozilla before 1.7.6 do not sufficiently address all attack vectors for loading chrome files and hijacking drag and drop events, which allows remote attackers to execute arbitrary XUL code by tricking a user into dragging a scrollbar, a variant of CVE-2005-0527, aka "Firescrolling 2."
CVE-2005-0402	Firefox before 1.0.2 allows remote attackers to execute arbitrary code by tricking a user into saving a page as a Firefox sidebar panel, then using the sidebar panel to inject Javascript into a privileged page.
CVE-2005-0527	Firefox 1.0 allows remote attackers to execute arbitrary code via plugins that load "privileged content" into frames, as demonstrated using certain XUL events when a user drags a scrollbar two times, aka "Firescrolling."
CVE-2005-0578	Firefox before 1.0.1 and Mozilla Suite before 1.7.6 use a predictable filename for the plugin temporary directory, which allows local users to delete arbitrary files of other users via a symlink attack on the plugtmp directory.
CVE-2005-0584	Firefox before 1.0.1 and Mozilla before 1.7.6, when displaying the HTTP Authentication dialog, do not change the focus to the tab that generated the prompt, which could facilitate spoofing and phishing attacks.

CVE-2005-0585	Firefox before 1.0.1 and Mozilla before 1.7.6 truncates long sub-domains or paths for display, which may allow remote malicious web sites to spoof legitimate sites and facilitate phishing attacks.
CVE-2005-0586	Firefox before 1.0.1 and Mozilla before 1.7.6 allows remote malicious web sites to spoof the extensions of files to download via the Content-Disposition header, which could be used to trick users into downloading dangerous content.
CVE-2005-0587	Firefox before 1.0.1 and Mozilla before 1.7.6 allows remote malicious web sites to overwrite arbitrary files by tricking the user into downloading a .LNK (link) file twice, which overwrites the file that was referenced in the first LNK file.
CVE-2005-0588	Firefox before 1.0.1 and Mozilla before 1.7.6 does not restrict xsl:include and xsl:import tags in XSLT stylesheets to the current domain, which allows remote attackers to determine the existence of files on the local system.
CVE-2005-0589	The Form Fill feature in Firefox before 1.0.1 allows remote attackers to steal potentially sensitive information via an input control that monitors the values that are generated by the autocomplete capability.
CVE-2005-0591	Firefox before 1.0.1 allows remote attackers to spoof the (1) security and (2) download modal dialog boxes, which could be used to trick users into executing script or downloading and executing a file, aka "Firespoofing."
CVE-2005-0592	Heap-based buffer overflow in the UTF8ToNewUnicode function for Firefox before 1.0.1 and Mozilla before 1.7.6 might allow remote attackers to cause a denial of service (crash) or execute arbitrary code via invalid sequences in a UTF8 encoded string that result in a zero length value.
CVE-2005-0593	Firefox before 1.0.1 and Mozilla before 1.7.6 allows remote attackers to spoof the SSL "secure site" lock icon via (1) a web site that does not finish loading, which shows the lock of the previous site, (2) a non-HTTP server that uses SSL, which causes the lock to be displayed when the SSL handshake is completed, or (3) a URL that generates an HTTP 204 error, which updates the icon and location information but does not change the display of the original site.
CVE-2005-0752	The Plugin Finder Service (PFS) in Firefox before 1.0.3 allows remote attackers to execute arbitrary code via a javascript: URL in the PLUGINSPAGE attribute of an EMBED tag.
CVE-2005-0989	The find_replen function in jsstr.c in the Javascript engine for Mozilla Suite 1.7.6, Firefox 1.0.1 and 1.0.2, and Netscape 7.2 allows remote attackers to read portions of heap memory in a Javascript string via the lambda replace method.
CVE-2005-1153	Firefox before 1.0.3 and Mozilla Suite before 1.7.7, when blocking a popup, allows remote attackers to execute arbitrary code via a javascript: URL that is executed when the user selects the "Show javascript" option.
CVE-2005-1154	Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to execute arbitrary script in other domains via a setter function for a variable in the target domain, which is executed when the user visits that domain, aka "Cross-site scripting through global scope pollution."
CVE-2005-1155	The favicon functionality in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to execute arbitrary code via a <LINK rel="icon"> tag with a javascript: URL in the href attribute, aka "Firelinking."
CVE-2005-1156	Firefox before 1.0.3, Mozilla Suite before 1.7.7, and Netscape 7.2 allows remote attackers to execute arbitrary script and code via a new search plugin using sidebar.addSearchEngine, aka "Firesearching 1."
CVE-2005-1157	Firefox before 1.0.3, Mozilla Suite before 1.7.7, and Netscape 7.2 allows remote attackers to replace existing search plugins with malicious ones using sidebar.addSearchEngine and the same filename as the target engine, which may not be displayed in the GUI, which could then be used to execute malicious script, aka "Firesearching 2."
CVE-2005-1158	Multiple "missing security checks" in Firefox before 1.0.3 allow remote attackers to inject arbitrary Javascript into privileged pages using the _search target of the Firefox sidebar.
CVE-2005-1159	The native implementations of InstallTrigger and other functions in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 do not properly verify the types of objects being accessed, which causes the Javascript interpreter to continue execution at the wrong memory address, which may allow attackers to cause a denial of service (application crash) and possibly execute arbitrary code by passing objects of the wrong type.
CVE-2005-1160	The privileged "chrome" UI code in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to gain privileges by overriding certain properties or methods of DOM nodes, as demonstrated using multiple attacks involving the eval function or the Script object.
CVE-2005-1476	Firefox 1.0.3 allows remote attackers to execute arbitrary Javascript in other domains by using an IFRAME and causing the browser to navigate to a previous javascript: URL, which can lead to arbitrary code execution when combined with CVE-2005-1477.
CVE-2005-1477	The install function in Firefox 1.0.3 allows remote web sites on the browser's whitelist, such as update.mozilla.org or addon.mozilla.org, to execute arbitrary Javascript with chrome privileges, leading to arbitrary code execution on the system when combined with vulnerabilities such as CVE-2005-1476, as demonstrated using a javascript: URL as the package icon and a cross-site scripting (XSS) attack on a vulnerable whitelist site.
CVE-2005-1531	Firefox before 1.0.4 and Mozilla Suite before 1.7.8 does not properly implement certain security checks for script injection, which allows remote attackers to execute script via "Wrapped" javascript: URLs, as demonstrated using (1) a javascript: URL in a view-source: URL, (2) a javascript: URL in a jar: URL, or (3) "a nested variant."
CVE-2005-1532	Firefox before 1.0.4 and Mozilla Suite before 1.7.8 do not properly limit privileges of Javascript eval and Script objects in the calling context, which allows remote attackers to conduct unauthorized activities via "non-DOM property overrides," a variant of CVE-2005-1160.

CVE-2005-1575	The file download dialog in Mozilla Firefox 0.10.1 and 1.0 for Windows allows remote attackers to hide the real file types of downloaded files via the Content-Type HTTP header and a filename containing whitespace, dots, or ASCII byte 160.
CVE-2005-1576	The file download dialog in Mozilla Firefox 0.10.1 and 1.0 for Windows uses the Content-Type HTTP header to determine the file type, but saves the original file extension when "Save to Disk" is selected, which allows remote attackers to hide the real file types of downloaded files.
CVE-2005-1937	A regression error in Firefox 1.0.3 and Mozilla 1.7.7 allows remote attackers to inject arbitrary Javascript from one page into the frameset of another site, aka the frame injection spoofing vulnerability, a re-introduction of a vulnerability that was originally identified and addressed by CVE-2004-0718.
CVE-2005-2114	Mozilla 1.7.8, Firefox 1.0.4, Camino 0.8.4, Netscape 8.0.2, and K-Meleon 0.9, and possibly other products that use the Gecko engine, allow remote attackers to cause a denial of service (application crash) via JavaScript that repeatedly calls an empty function.
CVE-2005-2260	The browser user interface in Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 and 7.2 does not properly distinguish between user-generated events and untrusted synthetic events, which makes it easier for remote attackers to perform dangerous actions that normally could only be performed manually by the user.
CVE-2005-2262	Firefox 1.0.3 and 1.0.4, and Netscape 8.0.2, allows remote attackers to execute arbitrary code by tricking the user into using the "Set As Wallpaper" (in Firefox) or "Set as Background" (in Netscape) context menu on an image URL that is really a javascript: URL with an eval statement, aka "Firewalling."
CVE-2005-2263	The InstallTrigger.install method in Firefox before 1.0.5 and Mozilla before 1.7.9 allows remote attackers to execute a callback function in the context of another domain by forcing a page navigation after the install method has been called, which causes the callback to be run in the context of the new page and results in a same origin violation.
CVE-2005-2264	Firefox before 1.0.5 allows remote attackers to steal sensitive information by opening a malicious link in the Firefox sidebar using the _search target, then injecting script into other pages via a data: URL.
CVE-2005-2265	Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 and 7.2 allows remote attackers to cause a denial of service (access violation and crash), and possibly execute arbitrary code, by calling InstallVersion.compareTo with an object instead of a string.
CVE-2005-2266	Firefox before 1.0.5 and Mozilla before 1.7.9 allows a child frame to call top.focus and other methods in a parent frame, even when the parent is in a different domain, which violates the same origin policy and allows remote attackers to steal sensitive information such as cookies and passwords from web sites whose child frames do not verify that they are in the same domain as their parents.
CVE-2005-2267	Firefox before 1.0.5 allows remote attackers to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL, which is run in the context of the previous page, and may lead to code execution if the standalone application loads a privileged chrome: URL.
CVE-2005-2268	Firefox before 1.0.5 and Mozilla before 1.7.9 does not clearly associate a Javascript dialog box with the web page that generated it, which allows remote attackers to spoof a dialog box from a trusted site and facilitates phishing attacks, aka the "Dialog Origin Spoofing Vulnerability."
CVE-2005-2269	Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 does not properly verify the associated types of DOM node names within the context of their namespaces, which allows remote attackers to modify certain tag properties, possibly leading to execution of arbitrary script or code, as demonstrated using an XHTML document with IMG tags with custom properties ("XHTML node spoofing").
CVE-2005-2270	Firefox before 1.0.5 and Mozilla before 1.7.9 does not properly clone base objects, which allows remote attackers to execute arbitrary code by navigating the prototype chain to reach a privileged object.
CVE-2005-2395	Mozilla Firefox 1.0.4 and 1.0.5 does not choose the challenge with the strongest authentication scheme available as required by RFC2617, which might cause credentials to be sent in plaintext even if an encrypted channel is available.
CVE-2005-2429	Firefox, when opening Microsoft Word documents, does not properly set the permissions on shared sections, which allows remote attackers to write arbitrary data to open applications in Microsoft Office.
CVE-2005-2701	Heap-based buffer overflow in Firefox before 1.0.7 and Mozilla Suite before 1.7.12 allows remote attackers to execute arbitrary code via an XBM image file that ends in a large number of spaces instead of the expected end tag.
CVE-2005-2702	Firefox before 1.0.7 and Mozilla Suite before 1.7.12 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via Unicode sequences with "zero-width non-joiner" characters.
CVE-2005-2703	Firefox before 1.0.7 and Mozilla Suite before 1.7.12 allows remote attackers to modify HTTP headers of XML HTTP requests via XMLHttpRequest, and possibly use the client to exploit vulnerabilities in servers or proxies, including HTTP request smuggling and HTTP request splitting.
CVE-2005-2704	Firefox before 1.0.7 and Mozilla Suite before 1.7.12 allows remote attackers to spoof DOM objects via an XBL control that implements an internal XPCOM interface.
CVE-2005-2705	Integer overflow in the JavaScript engine in Firefox before 1.0.7 and Mozilla Suite before 1.7.12 might allow remote attackers to execute arbitrary code.
CVE-2005-2706	Firefox before 1.0.7 and Mozilla before Suite 1.7.12 allows remote attackers to execute Javascript with chrome privileges via an about: page such as about:mozilla.

CVE-2005-2707	Firefox before 1.0.7 and Mozilla Suite before 1.7.12 allows remote attackers to spawn windows without user interface components such as the address and status bar, which could be used to conduct spoofing or phishing attacks.
CVE-2005-2871	Buffer overflow in the International Domain Name (IDN) support in Mozilla Firefox 1.0.6 and earlier, and Netscape 8.0.3.3 and 7.2, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a hostname with all "soft" hyphens (character 0xAD), which is not properly handled by the NormalizeIDN call in nsStandardURL::BuildNormalizedSpec.
CVE-2005-2968	Firefox 1.0.6 and Mozilla 1.7.10 allows attackers to execute arbitrary commands via shell metacharacters in a URL that is provided to the browser on the command line, which is sent unfiltered to bash.
CVE-2005-3089	Firefox 1.0.6 allows attackers to cause a denial of service (crash) via a Proxy Auto-Config (PAC) script that uses an eval statement. NOTE: it is not clear whether an untrusted party has any role in triggering this issue, so it might not be a vulnerability.
CVE-2005-4134	Mozilla Firefox 1.5, Netscape 8.0.4 and 7.2, and K-Meleon before 0.9.12 allows remote attackers to cause a denial of service (CPU consumption and delayed application startup) via a web site with a large title, which is recorded in history.dat but not processed efficiently during startup. NOTE: despite initial reports, the Mozilla vendor does not believe that this issue can be used to trigger a crash or buffer overflow in Firefox. Also, it has been independently reported that Netscape 8.1 does not have this issue.
CVE-2005-4685	Firefox and Mozilla can associate a cookie with multiple domains when the DNS resolver has a non-root domain in its search list, which allows remote attackers to trick a user into accepting a cookie for a hostname formed via search-list expansion of the hostname entered by the user, or steal a cookie for an expanded hostname, as demonstrated by an attacker who operates an ap1.com Internet web site to steal cookies associated with an ap1.com.example.com intranet web site.
CVE-2005-4720	Mozilla Firefox 1.0.7 and earlier on Linux allows remote attackers to cause a denial of service (client crash) via an IFRAME element with a large value of the WIDTH attribute, which triggers a problem related to representation of floating-point numbers, leading to an infinite loop of widget resizes and a corresponding large number of function calls on the stack.
CVE-2006-0292	The Javascript interpreter (jsinterp.c) in Mozilla and Firefox before 1.5.1 does not properly dereference objects, which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via unknown attack vectors related to garbage collection.
CVE-2006-0293	The function allocation code (js_NewFunction in jsfun.c) in Firefox 1.5 allows attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via user-defined methods that trigger garbage collection in a way that operates on freed objects.
CVE-2006-0296	The XULDocument.persist function in Mozilla, Firefox before 1.5.0.1, and SeaMonkey before 1.0 does not validate the attribute name, which allows remote attackers to execute arbitrary Javascript by injecting RDF data into the user's localstore.rdf file.
CVE-2006-0298	The XML parser in Mozilla Firefox before 1.5.0.1 and SeaMonkey before 1.0 allows remote attackers to cause a denial of service (crash) and possibly read sensitive data via unknown attack vectors that trigger an out-of-bounds read.
CVE-2006-0496	Cross-site scripting (XSS) vulnerability in Mozilla 1.7.12 and possibly earlier, Mozilla Firefox 1.0.7 and possibly earlier, and Netscape 8.1 and possibly earlier, allows remote attackers to inject arbitrary web script or HTML via the -moz-binding (Cascading Style Sheets) CSS property, which does not require that the style sheet have the same origin as the web page, as demonstrated by the compromise of a large number of LiveJournal accounts.
CVE-2006-1273	** DISPUTED ** Mozilla Firefox 1.0.7 and 1.5.0.1 allows remote attackers to cause a denial of service (crash) via an HTML tag with a large number of script action handlers such as onload and onmouseover, which triggers the crash when the user views the page source. NOTE: Red Hat has disputed this issue, suggesting that "It is likely the reporter was running the IE Tab extension," and Mozilla also confirmed that this is not an issue in Firefox itself.
CVE-2006-1650	Firefox 1.5.0.1 allows remote attackers to spoof the address bar and possibly conduct phishing attacks by re-opening the window to a malicious Shockwave Flash application, then changing the window location back to a trusted URL while the Flash application is still loading. NOTE: a followup was unable to replicate this issue.
CVE-2006-1790	A regression fix in Mozilla Firefox 1.0.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the InstallTrigger.install method, which leads to memory corruption.
CVE-2006-1942	Mozilla Firefox 1.5.0.2 and possibly other versions before 1.5.0.4, Netscape 8.1, 8.0.4, and 7.2, and K-Meleon 0.9.13 allows user-assisted remote attackers to open local files via a web page with an IMG element containing a SRC attribute with a non-image file:// URL, then tricking the user into selecting View Image for the broken image, as demonstrated using a .wma file to launch Windows Media Player, or by referencing an "alternate web page."
CVE-2006-1993	Mozilla Firefox 1.5.0.2, when designMode is enabled, allows remote attackers to cause a denial of service and possibly execute arbitrary code via certain Javascript that is not properly handled by the contentWindow.focus method in an iframe, which causes a reference to a deleted controller context object. NOTE: this was originally claimed to be a buffer overflow in (1) js320.dll and (2) xpcom_core.dll, but the vendor disputes this claim.
CVE-2006-2057	Argument injection vulnerability in Mozilla Firefox 1.0.6 allows user-assisted remote attackers to modify command line arguments to an invoked mail client via " (double quote) characters in a mailto: scheme handler, as

	demonstrated by launching Microsoft Outlook with an arbitrary filename as an attachment. NOTE: it is not clear whether this issue is implementation-specific or a problem in the Microsoft API.
CVE-2006-2332	Mozilla Firefox 1.5.0.3 allows remote attackers to cause a denial of service via a web page with a large number of IMG elements in which the SRC attribute is a mailto URI. NOTE: another researcher found that the web page caused a temporary browser slowdown instead of a crash.
CVE-2006-2538	IE Tab 1.0.9 plugin for Mozilla Firefox 1.5.0.3 allows remote user-assisted attackers to cause a denial of service (application crash), possibly due to a null dereference, via certain Javascript, as demonstrated using a url parameter to the content/reloaded.html page in a chrome:// URI. Some third-party researchers claim that they are unable to reproduce this vulnerability.
CVE-2006-2613	Mozilla Suite 1.7.13, Mozilla Firefox 1.5.0.3 and possibly other versions before before 1.8.0, and Netscape 7.2 and 8.1, and possibly other versions and products, allows remote user-assisted attackers to obtain information such as the installation path by causing exceptions to be thrown and checking the message contents.
CVE-2006-2723	Unspecified versions of Mozilla Firefox allow remote attackers to cause a denial of service (crash) via a web page that contains a large number of nested marquee tags. NOTE: a followup post indicated that the initial report could not be verified.
CVE-2006-2777	Unspecified vulnerability in Mozilla Firefox before 1.5.0.4 and SeaMonkey before 1.0.2 allows remote attackers to execute arbitrary code by using the nsISelectionPrivate interface of the Selection object to add a SelectionListener and create notifications that are executed in a privileged context.
CVE-2006-2782	Firefox 1.5.0.2 does not fix all test cases associated with CVE-2006-1729, which allows remote attackers to read arbitrary files by inserting the target filename into a text box, then turning that box into a file upload control.
CVE-2006-2784	The PLUGINSPAGE functionality in Mozilla Firefox before 1.5.0.4 allows remote user-assisted attackers to execute privileged code by tricking a user into installing missing plugins and selecting the "Manual Install" button, then using nested javascript: URLs. NOTE: the manual install button is used for downloading software from a remote web site, so this issue would not cross privilege boundaries if the user progresses to the point of installing malicious software from the attacker-controlled site.
CVE-2006-2785	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 1.5.0.4 allows user-assisted remote attackers to inject arbitrary web script or HTML by tricking a user into (1) performing a "View Image" on a broken image in which the SRC attribute contains a Javascript URL, or (2) selecting "Show only this frame" on a frame whose SRC attribute contains a Javascript URL.
CVE-2006-2788	Double free vulnerability in the getRawDER function for nsIX509Cert in Firefox allows remote attackers to cause a denial of service (hang) and possibly execute arbitrary code via certain Javascript code.
CVE-2006-2894	Mozilla Firefox 1.5.0.4, 2.0.x before 2.0.0.8, Mozilla Suite 1.7.13, Mozilla SeaMonkey 1.0.2 and other versions before 1.1.5, and Netscape 8.1 and earlier allow user-assisted remote attackers to read arbitrary files by tricking a user into typing the characters of the target filename in a text box and using the OnKeyDown, OnKeyPress, and OnKeyUp Javascript keystroke events to change the focus and cause those characters to be inserted into a file upload input control, which can then upload the file when the user submits the form.
CVE-2006-3352	** DISPUTED ** Cross-domain vulnerability in Mozilla Firefox allows remote attackers to access restricted information from other domains via an object tag with a data parameter that references a link on the attacker's originating site that specifies a Location HTTP header that references the target site, which then makes that content available through the outerHTML attribute of the object. NOTE: this description was based on a report that has since been retracted by the original authors. The authors misinterpreted their test results. Other third parties also disputed the original report. Therefore, this is not a vulnerability. It is being assigned a candidate number to provide a clear indication of its status.
CVE-2006-3677	Mozilla Firefox 1.5 before 1.5.0.5 and SeaMonkey before 1.0.3 allows remote attackers to execute arbitrary code by changing certain properties of the window navigator object (window.navigator) that are accessed when Java starts up, which causes a crash that leads to code execution.
CVE-2006-3731	Mozilla Firefox 1.5.0.4 and earlier allows remote user-assisted attackers to cause a denial of service (crash) via a form with a multipart/form-data encoding and a user-uploaded file. NOTE: a third party has claimed that this issue might be related to the LiveHTTPHeaders extension.
CVE-2006-3801	Mozilla Firefox 1.5 before 1.5.0.5 and SeaMonkey before 1.0.3 does not properly clear a JavaScript reference to a frame or window, which leaves a pointer to a deleted object that allows remote attackers to execute arbitrary native code.
CVE-2006-3808	Mozilla Firefox before 1.5.0.5 and SeaMonkey before 1.0.3 allows remote Proxy AutoConfig (PAC) servers to execute code with elevated privileges via a PAC script that sets the FindProxyForURL function to an eval method on a privileged object.
CVE-2006-4253	Concurrency vulnerability in Mozilla Firefox 1.5.0.6 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via multiple Javascript timed events that load a deeply nested XML file, followed by redirecting the browser to another page, which leads to a concurrency failure that causes structures to be freed incorrectly, as demonstrated by (1) ffoxdie and (2) ffoxdie3. NOTE: it has been reported that Netscape 8.1 and K-Meleon 1.0.1 are also affected by ffoxdie. Mozilla confirmed to CVE that ffoxdie and ffoxdie3 trigger the same underlying vulnerability. NOTE: it was later reported that Firefox 2.0 RC2 and 1.5.0.7 are also affected.

CVE-2006-4310	Mozilla Firefox 1.5.0.6 allows remote attackers to cause a denial of service (crash) via a crafted FTP response, when attempting to connect with a username and password via the FTP URI.
CVE-2006-4561	Mozilla Firefox 1.5.0.6 allows remote attackers to execute arbitrary JavaScript in the context of the browser's session with an arbitrary intranet web server, by hosting script on an Internet web server that can be made inaccessible by the attacker and that has a domain name under the attacker's control, which can force the browser to drop DNS pinning and perform a new DNS query for the domain name after the script is already running.
CVE-2006-4568	Mozilla Firefox before 1.5.0.7 and SeaMonkey before 1.0.5 allows remote attackers to bypass the security model and inject content into the sub-frame of another site via targetWindow.frames[n].document.open(), which facilitates spoofing and other attacks.
CVE-2006-4569	The popup blocker in Mozilla Firefox before 1.5.0.7 opens the "blocked popups" display in the context of the Location bar instead of the subframe from which the popup originated, which might make it easier for remote user-assisted attackers to conduct cross-site scripting (XSS) attacks.
CVE-2006-5159	** DISPUTED ** Stack-based buffer overflow in Mozilla Firefox allows remote attackers to execute arbitrary code via unspecified vectors involving JavaScript. NOTE: the vendor and original researchers have released a follow-up comment disputing the severity of this issue, in which the researcher states that "we mentioned that there was a previously known Firefox vulnerability that could result in a stack overflow ending up in remote code execution. However, the code we presented did not in fact do this... I have not succeeded in making this code do anything more than cause a crash and eat up system resources".
CVE-2006-5160	** DISPUTED ** Multiple unspecified vulnerabilities in Mozilla Firefox have unspecified vectors and impact, as claimed during ToorCon 2006. NOTE: the vendor and original researchers have released a follow-up comment disputing this issue, in which one researcher states that "I have no undisclosed Firefox vulnerabilities. The person who was speaking with me made this claim, and I honestly have no idea if he has them or not."
CVE-2006-5633	Firefox 1.5.0.7 and 2.0, and Seamonkey 1.1b, allows remote attackers to cause a denial of service (crash) by creating a range object using createRange, calling selectNode on a DocType node (DOCUMENT_TYPE_NODE), then calling createContextualFragment on the range, which triggers a null dereference. NOTE: the original Bugtraq post mentioned that code execution was possible, but followup analysis has shown that it is only a null dereference.
CVE-2006-5783	** DISPUTED ** Firefox 1.5.0.7 on Kubuntu Linux allows remote attackers to cause a denial of service (crash) via a long URL in an A tag. NOTE: this issue has been disputed by several vendors, who could not reproduce the report. In addition, the scope of the impact - system freeze - suggests an issue that is not related to Firefox. Due to this impact, CVE concurs with the dispute.
CVE-2006-6077	The (1) Password Manager in Mozilla Firefox 2.0, and 1.5.0.8 and earlier; and the (2) Passcard Manager in Netscape 8.1.2 and possibly other versions, do not properly verify that an ACTION URL in a FORM element containing a password INPUT element matches the web site for which the user stored a password, which allows remote attackers to obtain passwords via a password INPUT element on a different web page located on the web site intended for this password.
CVE-2006-6506	The "Feed Preview" feature in Mozilla Firefox 2.0 before 2.0.0.1 sends the URL of the feed when requesting favicon.ico icons, which results in a privacy leak that might allow feed viewing services to determine browsing habits.
CVE-2006-6507	Mozilla Firefox 2.0 before 2.0.0.1 allows remote attackers to bypass Cross-Site Scripting (XSS) protection via vectors related to a Function.prototype regression error.
CVE-2006-6585	The Extensions manager in Mozilla Firefox 2.0 does not properly populate the list of local extensions, which allows attackers to construct an extension that hides itself by finding its name in the list and then calling RemoveElement, as demonstrated by the FFsniFF extension. NOTE: it was later reported that 3.0 is also affected.
CVE-2006-6971	Mozilla Firefox 2.0, possibly only when running on Windows, allows remote attackers to bypass the Phishing Protection mechanism by representing an IP address in (1) dotted-hex, (2) dotted-octal, (3) single decimal integer, (4) single hex integer, or (5) single octal integer format, which is not captured by the blacklist filter.
CVE-2007-0778	The page cache feature in Mozilla Firefox before 1.5.0.10 and 2.x before 2.0.0.2, and SeaMonkey before 1.0.8 can generate hash collisions that cause page data to be appended to the wrong page cache, which allows remote attackers to obtain sensitive information or enable further attack vectors when the target page is reloaded from the cache.
CVE-2007-0779	GUI overlay vulnerability in Mozilla Firefox 1.5.x before 1.5.0.10 and 2.x before 2.0.0.2, and SeaMonkey before 1.0.8 allows remote attackers to spoof certain user interface elements, such as the host name or security indicators, via the CSS3 hotspot property with a large, transparent, custom cursor.
CVE-2007-0780	browser.js in Mozilla Firefox 1.5.x before 1.5.0.10 and 2.x before 2.0.0.2, and SeaMonkey before 1.0.8 uses the requesting URI to identify child windows, which allows remote attackers to conduct cross-site scripting (XSS) attacks by opening a blocked popup originating from a javascript: URI in combination with multiple frames having the same data: URI.
CVE-2007-0800	Cross-zone vulnerability in Mozilla Firefox 1.5.0.9 considers blocked popups to have an internal zone origin, which allows user-assisted remote attackers to cross zone restrictions and read arbitrary file:// URIs by convincing a user to show a blocked popup.

CVE-2007-0801	The nsExternalAppHandler::SetUpTempFile function in Mozilla Firefox 1.5.0.9 creates temporary files with predictable filenames based on creation time, which allows remote attackers to execute arbitrary web script or HTML via a crafted XMLHttpRequest.
CVE-2007-0802	Mozilla Firefox 2.0.0.1 allows remote attackers to bypass the Phishing Protection mechanism by adding certain characters to the end of the domain name, as demonstrated by the "." and "/" characters, which is not caught by the Phishing List blacklist filter.
CVE-2007-0896	Cross-site scripting (XSS) vulnerability in the (1) Sage before 1.3.10, and (2) Sage++ extensions for Firefox, allows remote attackers to inject arbitrary web script or HTML via a "<SCRIPT/=SRC=" sequence in an RSS feed, a different vulnerability than CVE-2006-4712.
CVE-2007-0981	Mozilla based browsers, including Firefox before 1.5.0.10 and 2.x before 2.0.0.2, and SeaMonkey before 1.0.8, allow remote attackers to bypass the same origin policy, steal cookies, and conduct other attacks by writing a URI with a null byte to the hostname (location.hostname) DOM property, due to interactions with DNS resolver code.
CVE-2007-0994	A regression error in Mozilla Firefox 2.x before 2.0.0.2 and 1.x before 1.5.0.10, and SeaMonkey 1.1 before 1.1.1 and 1.0 before 1.0.8, allows remote attackers to execute arbitrary JavaScript as the user via an HTML mail message with a javascript: URI in an (1) img, (2) link, or (3) style tag, which bypasses the access checks and executes code with chrome privileges.
CVE-2007-0995	Mozilla Firefox before 1.5.0.10 and 2.x before 2.0.0.2, and SeaMonkey before 1.0.8 ignores trailing invalid HTML characters in attribute names, which allows remote attackers to bypass content filters that use regular expressions.
CVE-2007-0996	The child frames in Mozilla Firefox before 1.5.0.10 and 2.x before 2.0.0.2, and SeaMonkey before 1.0.8 inherit the default charset from the parent window, which allows remote attackers to conduct cross-site scripting (XSS) attacks, as demonstrated using the UTF-7 character set.
CVE-2007-1004	Mozilla Firefox might allow remote attackers to conduct spoofing and phishing attacks by writing to an about:blank tab and overlaying the location bar.
CVE-2007-1084	Mozilla Firefox 2.0.0.1 and earlier does not prompt users before saving bookmarklets, which allows remote attackers to bypass the same-domain policy by tricking a user into saving a bookmarklet with a data: scheme, which is executed in the context of the last visited web page.
CVE-2007-1092	Mozilla Firefox 1.5.0.9 and 2.0.0.1, and SeaMonkey before 1.0.8 allow remote attackers to execute arbitrary code via JavaScript onUnload handlers that modify the structure of a document, which triggers memory corruption due to the lack of a finalize hook on DOM window objects.
CVE-2007-1095	Mozilla Firefox before 2.0.0.8 and SeaMonkey before 1.1.5 do not properly implement JavaScript onUnload handlers, which allows remote attackers to run certain JavaScript code and access the location DOM hierarchy in the context of the next web site that is visited by a client.
CVE-2007-1116	The CheckLoadURI function in Mozilla Firefox 1.8 lists the about: URI as a ChromeProtocol and can be loaded via JavaScript, which allows remote attackers to obtain sensitive information by querying the browser's session history.
CVE-2007-1256	Mozilla Firefox 2.0.0.2 allows remote attackers to spoof the address bar, favicons, and document source, and perform updates in the context of arbitrary websites, by repeatedly setting document.location in the onunload attribute when linking to another website, a variant of CVE-2007-1092.
CVE-2007-1362	Mozilla Firefox 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, allows remote attackers to cause a denial of service via (1) a large cookie path parameter, which triggers memory consumption, or (2) an internal delimiter within cookie path or name values, which could trigger a misinterpretation of cookie data, aka "Path Abuse in Cookies."
CVE-2007-1377	AcroPDF.DLL in Adobe Reader 8.0, when accessed from Mozilla Firefox, Netscape, or Opera, allows remote attackers to cause a denial of service (unspecified resource consumption) via a .pdf URL with an anchor identifier that begins with search= followed by many %n sequences, a different vulnerability than CVE-2006-6027 and CVE-2006-6236.
CVE-2007-1562	The FTP protocol implementation in Mozilla Firefox before 1.5.0.11 and 2.x before 2.0.0.3 allows remote attackers to force the client to connect to other servers, perform a proxied port scan, or obtain sensitive information by specifying an alternate server address in an FTP PASV response.
CVE-2007-1736	Mozilla Firefox 2.0.0.3 does not check URLs embedded in (1) object or (2) iframe HTML tags against the phishing site blacklist, which allows remote attackers to bypass phishing protection.
CVE-2007-1762	Mozilla Firefox 2.0.0.1 through 2.0.0.3 does not canonicalize URLs before checking them against the phishing site blacklist, which allows remote attackers to bypass phishing protection via multiple / (slash) characters in the URL.
CVE-2007-1970	Mozilla Firefox does not warn the user about HTTP elements on an HTTPS page when the HTTP elements are dynamically created by a delayed document.write, which allows remote attackers to supply unauthenticated content and conduct phishing attacks.
CVE-2007-2162	(1) Mozilla Firefox 2.0.0.3 and (2) GNU IceWeasel 2.0.0.3 allow remote attackers to cause a denial of service (browser crash or system hang) via JavaScript that matches a regular expression against a long string, as demonstrated using /(./)*/.
CVE-2007-2176	Unspecified vulnerability in Mozilla Firefox allows remote attackers to execute arbitrary code via unspecified vectors involving Javascript errors. NOTE: this might be the same issue as CVE-2007-2175.

CVE-2007-2292	CRLF injection vulnerability in the Digest Authentication support for Mozilla Firefox before 2.0.0.8 and SeaMonkey before 1.1.5 allows remote attackers to conduct HTTP request splitting attacks via LF (%0a) bytes in the username attribute.
CVE-2007-2671	Mozilla Firefox 2.0.0.3 allows remote attackers to cause a denial of service (application crash) via a long hostname in an HREF attribute in an A element, which triggers an out-of-bounds memory access.
CVE-2007-2869	The form autocomplete feature in Mozilla Firefox 1.5.x before 1.5.0.12, 2.x before 2.0.0.4, and possibly earlier versions, allows remote attackers to cause a denial of service (persistent temporary CPU consumption) via a large number of characters in a submitted form.
CVE-2007-2870	Mozilla Firefox 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, allows remote attackers to bypass the same-origin policy and conduct cross-site scripting (XSS) and other attacks by using the addEventListener method to add an event listener for a site, which is executed in the context of that site.
CVE-2007-2871	Mozilla Firefox 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, allows remote attackers to spoof or hide the browser chrome, such as the location bar, by placing XUL popups outside of the browser's content pane. NOTE: this issue can be leveraged for phishing and other attacks.
CVE-2007-3072	Directory traversal vulnerability in Mozilla Firefox before 2.0.0.4 on Windows allows remote attackers to read arbitrary files via ..%5C (dot dot encoded backslash) sequences in a resource:// URI.
CVE-2007-3073	Directory traversal vulnerability in Mozilla Firefox 2.0.0.4 and earlier on Mac OS X and Unix allows remote attackers to read arbitrary files via ..%2F (dot dot encoded slash) sequences in a resource:// URI.
CVE-2007-3074	Mozilla Firefox 2.0.0.4 and earlier allows remote attackers to read files in the local Firefox installation directory via a resource:// URI.
CVE-2007-3089	Mozilla Firefox before 2.0.0.5 does not prevent use of document.write to replace an IFRAME (1) during the load stage or (2) in the case of an about:blank frame, which allows remote attackers to display arbitrary HTML or execute certain JavaScript code, as demonstrated by code that intercepts keystroke values from window.event, aka the "promiscuous IFRAME access bug," a related issue to CVE-2006-4568.
CVE-2007-3285	Mozilla Firefox before 2.0.0.5, when run on Windows, allows remote attackers to bypass file type checks and possibly execute programs via a (1) file:/// or (2) resource: URI with a dangerous extension, followed by a NULL byte (%00) and a safer extension, which causes Firefox to treat the requested file differently than Windows would.
CVE-2007-3511	The focus handling for the onkeydown event in Mozilla Firefox 1.5.0.12, 2.0.0.4 and other versions before 2.0.0.8, and SeaMonkey before 1.1.5 allows remote attackers to change field focus and copy keystrokes via the "for" attribute in a label, which bypasses the focus prevention, as demonstrated by changing focus from a textarea to a file upload field.
CVE-2007-3656	Mozilla Firefox before 1.8.0.13 and 1.8.1.x before 1.8.1.5 does not perform a security zone check when processing a wyciwyg URI, which allows remote attackers to obtain sensitive information, poison the browser cache, and possibly enable further attack vectors via (1) HTTP 302 redirect controls, (2) XMLHttpRequest, or (3) view-source URIs.
CVE-2007-3657	** DISPUTED ** Mozilla Firefox 2.0.0.4 allows remote attackers to cause a denial of service by opening multiple tabs in a popup window. NOTE: this issue has been disputed by third party researchers, stating that "this does not crash on me, and I can't see a likely mechanism of action that would lead to a DoS condition."
CVE-2007-3670	Argument injection vulnerability in Microsoft Internet Explorer, when running on systems with Firefox installed and certain URIs registered, allows remote attackers to conduct cross-browser scripting attacks and execute arbitrary commands via shell metacharacters in a (1) FirefoxURL or (2) FirefoxHTML URI, which are inserted into the command line that is created when invoking firefox.exe. NOTE: it has been debated as to whether the issue is in Internet Explorer or Firefox. As of 20070711, it is CVE's opinion that IE appears to be failing to properly delimit the URL argument when invoking Firefox, and this issue could arise with other protocol handlers in IE as well. However, Mozilla has stated that it will address the issue with a "defense in depth" fix that will "prevent IE from sending Firefox malicious data."
CVE-2007-3736	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 2.0.0.5 allows remote attackers to inject arbitrary web script "into another site's context" via a "timing issue" involving the (1) addEventListener or (2) setTimeout function, probably by setting events that activate after the context has changed.
CVE-2007-3737	Mozilla Firefox before 2.0.0.5 allows remote attackers to execute arbitrary code with chrome privileges by calling an event handler from an unspecified "element outside of a document."
CVE-2007-3738	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.5 allow remote attackers to execute arbitrary code via a crafted XPCNativeWrapper.
CVE-2007-3827	Mozilla Firefox allows for cookies to be set with a null domain (aka "domainless cookies"), which allows remote attackers to pass information between arbitrary domains and track user activity, as demonstrated by the domain attribute in the document.cookie variable in a javascript: window.
CVE-2007-4013	Multiple unspecified vulnerabilities in (1) Net6Helper.DLL (aka Net6Launcher Class) 4.5.2 and earlier, (2) npCtxCAO.dll (aka Citrix Endpoint Analysis Client) in a Firefox plugin directory, and (3) a second npCtxCAO.dll (aka CCAOControl Object) before 4.5.0.0 in Citrix Access Gateway Standard Edition before 4.5.5 and Advanced Edition before 4.5 HF1 have unknown impact and attack vectors, possibly related to buffer overflows. NOTE: vector 3 might overlap CVE-2007-3679.

CVE-2007-4041	Multiple argument injection vulnerabilities in Mozilla Firefox 2.0.0.5 and 3.0alpha allow remote attackers to execute arbitrary commands via a NULL byte (%00) and shell metacharacters in a (1) mailto, (2) nntp, (3) news, (4) snews, or (5) telnet URI, a similar issue to CVE-2007-3670.
CVE-2007-4357	Mozilla Firefox 2.0.0.6 and earlier allows remote attackers to spoof the contents of the status bar via a link to a data: URI containing an encoded URL. NOTE: the severity of this issue has been disputed by a reliable third party, since the intended functionality of the status bar allows it to be modified.
CVE-2007-4879	Mozilla Firefox before Firefox 2.0.0.13, and SeaMonkey before 1.1.9, can automatically install TLS client certificates with minimal user interaction, and automatically sends these certificates when requested, which makes it easier for remote web sites to track user activities across domains by requesting the TLS client certificates from other domains.
CVE-2007-5045	Argument injection vulnerability in Apple QuickTime 7.1.5 and earlier, when running on systems with Mozilla Firefox before 2.0.0.7 installed, allows remote attackers to execute arbitrary commands via a QuickTime Media Link (QTL) file with an embed XML element and a qtnext parameter containing the Firefox "-chrome" argument. NOTE: this is a related issue to CVE-2006-4965 and the result of an incomplete fix for CVE-2007-3670.
CVE-2007-5274	Sun Java Runtime Environment (JRE) in JDK and JRE 6 Update 2 and earlier, JDK and JRE 5.0 Update 12 and earlier, SDK and JRE 1.4.2_15 and earlier, and SDK and JRE 1.3.1_20 and earlier, when Firefox or Opera is used, allows remote attackers to violate the security model for JavaScript outbound connections via a multi-pin DNS rebinding attack dependent on the LiveConnect API, in which JavaScript download relies on DNS resolution by the browser, but JavaScript socket operations rely on separate DNS resolution by a Java Virtual Machine (JVM), a different issue than CVE-2007-5273. NOTE: this is similar to CVE-2007-5232.
CVE-2007-5334	Mozilla Firefox before 2.0.0.8 and SeaMonkey before 1.1.5 can hide the window's titlebar when displaying XUL markup language documents, which makes it easier for remote attackers to conduct phishing and spoofing attacks by setting the hidechrome attribute.
CVE-2007-5335	Mozilla Firefox 2.0 before 2.0.0.8 allows remote attackers to obtain sensitive system information by using the addMicrosummaryGenerator sidebar method to access file: URIs.
CVE-2007-5337	Mozilla Firefox before 2.0.0.8 and SeaMonkey before 1.1.5, when running on Linux systems with gnome-vfs support, might allow remote attackers to read arbitrary files on SSH/sftp servers that accept key authentication by creating a web page on the target server, in which the web page contains URIs with (1) smb: or (2) sftp: schemes that access other files from the server.
CVE-2007-5338	Mozilla Firefox before 2.0.0.8 and SeaMonkey before 1.1.5 allow remote attackers to execute arbitrary Javascript with user privileges by using the Script object to modify XPCNativeWrappers in a way that causes the script to be executed when a chrome action is performed.
CVE-2007-5414	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 2.0, when UTF-7 document content is rendered directly in UTF-7, allows remote attackers to inject arbitrary web script or HTML via a gopher URI that uses single quote characters to delimit a literal string within an XSS sequence, a related issue to CVE-2007-5415.
CVE-2007-5415	Cross-site scripting (XSS) vulnerability in Mozilla Firefox 2.0, when UTF-7 document content is rendered directly in UTF-7, allows remote attackers to inject arbitrary web script or HTML via a gopher URI that uses '/' (slash) characters to delimit a literal string within an XSS sequence, a related issue to CVE-2007-5414.
CVE-2007-5459	Cross-site scripting (XSS) vulnerability in the sidebar HTML page in the MouseoverDictionary before 0.6.2 extension for Mozilla Firefox allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2007-5691	ParseFTPList.cpp in Mozilla Firefox 2.0.0.7 allows remote FTP servers to cause a denial of service (application crash) via a crafted reply to an unspecified listing command, related to "reading from invalid pointer."
CVE-2007-5896	Mozilla Firefox 2.0.0.9 allows remote attackers to cause a denial of service (CPU consumption and crash) via an iframe with Javascript that sets the document.location to contain a leading NULL byte (\x00) and a (1) res://, (2) about:config, or (3) file:/// URI.
CVE-2007-5947	The jar protocol handler in Mozilla Firefox before 2.0.0.10 and SeaMonkey before 1.1.7 retrieves the inner URL regardless of its MIME type, and considers HTML documents within a jar archive to have the same origin as the inner URL, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a jar: URI.
CVE-2007-5959	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.10 and SeaMonkey before 1.1.7 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors that trigger memory corruption.
CVE-2007-5960	Mozilla Firefox before 2.0.0.10 and SeaMonkey before 1.1.7 sets the Referer header to the window or frame in which script is running, instead of the address of the content that initiated the script, which allows remote attackers to spoof HTTP Referer headers and bypass Referer-based CSRF protection schemes by setting window.location and using a modal alert dialog that causes the wrong Referer to be sent.
CVE-2007-6589	The jar protocol handler in Mozilla Firefox before 2.0.0.10 and SeaMonkey before 1.1.7 does not update the origin domain when retrieving the inner URL parameter yields an HTTP redirect, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a jar: URI, a different vulnerability than CVE-2007-5947.
CVE-2007-6715	Mozilla Firefox allows remote attackers to cause a denial of service (crash) via crafted image, as demonstrated by the zzuf lol-firefox.gif test case.

CVE-2008-0016	Stack-based buffer overflow in the URL parsing implementation in Mozilla Firefox before 2.0.0.17 and SeaMonkey before 1.1.12 allows remote attackers to execute arbitrary code via a crafted UTF-8 URL in a link.
CVE-2008-0017	The http-index-format MIME type parser ( <code>nsDirIndexParser</code> ) in Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 does not check for an allocation failure, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an HTTP index response with a crafted 200 header, which triggers memory corruption and a buffer overflow.
CVE-2008-0367	Mozilla Firefox 2.0.0.11, 3.0b2, and possibly earlier versions, when prompting for HTTP Basic Authentication, displays the site requesting the authentication after the Realm text, which might make it easier for remote HTTP servers to conduct phishing and spoofing attacks.
CVE-2008-0414	Mozilla Firefox before 2.0.0.12 and SeaMonkey before 1.1.8 allows user-assisted remote attackers to trick the user into uploading arbitrary files via label tags that shift focus to a file input field, aka "focus spoofing."
CVE-2008-0417	CRLF injection vulnerability in Mozilla Firefox before 2.0.0.12 allows remote user-assisted web sites to corrupt the user's password store via newlines that are not properly handled when the user saves a password.
CVE-2008-0419	Mozilla Firefox before 2.0.0.12 and SeaMonkey before 1.1.8 allows remote attackers to steal navigation history and cause a denial of service (crash) via images in a page that uses designMode frames, which triggers memory corruption related to resize handles.
CVE-2008-0592	Mozilla Firefox before 2.0.0.12 and SeaMonkey before 1.1.8 allows user-assisted remote attackers to cause a denial of service via a plain .txt file with a "Content-Disposition: attachment" and an invalid "Content-Type: plain/text," which prevents Firefox from rendering future plain text files within the browser.
CVE-2008-0593	Gecko-based browsers, including Mozilla Firefox before 2.0.0.12 and SeaMonkey before 1.1.8, modify the <code>.href</code> property of stylesheet DOM nodes to the final URI of a 302 redirect, which might allow remote attackers to bypass the Same Origin Policy and read sensitive information from the original URL, such as with Single-Signon systems.
CVE-2008-0594	Mozilla Firefox before 2.0.0.12 does not always display a web forgery warning dialog if the entire contents of a web page are in a DIV tag that uses absolute positioning, which makes it easier for remote attackers to conduct phishing attacks.
CVE-2008-1238	Mozilla Firefox before 2.0.0.13 and SeaMonkey before 1.1.9, when generating the HTTP Referer header, does not list the entire URL when it contains Basic Authentication credentials without a username, which makes it easier for remote attackers to bypass application protection mechanisms that rely on Referer headers, such as with some Cross-Site Request Forgery (CSRF) mechanisms.
CVE-2008-1240	LiveConnect in Mozilla Firefox before 2.0.0.13 and SeaMonkey before 1.1.9 does not properly parse the content origin for jar: URIs before sending them to the Java plugin, which allows remote attackers to access arbitrary ports on the local machine. NOTE: this is closely related to CVE-2008-1195.
CVE-2008-1241	GUI overlay vulnerability in Mozilla Firefox before 2.0.0.13 and SeaMonkey before 1.1.9 allows remote attackers to spoof form elements and redirect user inputs via a borderless XUL pop-up window from a background tab.
CVE-2008-2014	Mozilla Firefox 3.0 beta 5 allows remote attackers to cause a denial of service (application crash) via JavaScript code that calls <code>document.write</code> in an infinite loop.
CVE-2008-2399	Directory traversal vulnerability in the FireFTP add-on before 0.98.20080518 for Firefox allows remote FTP servers to create or overwrite arbitrary files via ..\ (dot dot backslash) sequences in responses to (1) MLSD and (2) LIST commands, a related issue to CVE-2002-1345. NOTE: this can be leveraged for code execution by writing to a Startup folder.
CVE-2008-2419	Mozilla Firefox 2.0.0.14 allows remote attackers to cause a denial of service (heap corruption and application crash) or possibly execute arbitrary code by triggering an error condition during certain Iframe operations between a JSframe write and a JSframe close, as demonstrated by an error in loading an empty Java applet defined by a <code>'src="javascript:'</code> sequence.
CVE-2008-2786	Buffer overflow in Firefox 3.0 and 2.0.x has unknown impact and attack vectors. NOTE: due to lack of details as of 20080619, it is not clear whether this is the same issue as CVE-2008-2785. A CVE identifier has been assigned for tracking purposes.
CVE-2008-2800	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 allow remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via vectors involving (1) an event handler attached to an outer window, (2) a <code>SCRIPT</code> element in an unloaded document, or (3) the <code>onreadystatechange</code> handler in conjunction with an <code>XMLHttpRequest</code> .
CVE-2008-2801	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 do not properly implement JAR signing, which allows remote attackers to execute arbitrary code via (1) injection of JavaScript into documents within a JAR archive or (2) a JAR archive that uses relative URLs to JavaScript files.
CVE-2008-2805	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 allow remote attackers to force the upload of arbitrary local files from a client computer via vectors involving <code>originalTarget</code> and <code>DOM Range</code> .
CVE-2008-2807	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 do not properly handle an invalid .properties file for an add-on, which allows remote attackers to read uninitialized memory, as demonstrated by use of ISO 8859 encoding instead of UTF-8 encoding in a French .properties file.
CVE-2008-2809	Mozilla 1.9 M8 and earlier, Mozilla Firefox 2 before 2.0.0.15, SeaMonkey 1.1.5 and other versions before 1.1.10, Netscape 9.0, and other Mozilla-based web browsers, when a user accepts an SSL server certificate on the basis of

	the CN domain name in the DN field, regard the certificate as also accepted for all domain names in subjectAltName:dNSName fields, which makes it easier for remote attackers to trick a user into accepting an invalid certificate for a spoofed web site.
CVE-2008-2810	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 do not properly identify the context of Windows shortcut files, which allows user-assisted remote attackers to bypass the Same Origin Policy via a crafted web site for which the user has previously saved a shortcut.
CVE-2008-2933	Mozilla Firefox before 2.0.0.16, and 3.x before 3.0.1, interprets '\  (pipe) characters in a command-line URI as requests to open multiple tabs, which allows remote attackers to access chrome:i URIs, or read arbitrary local files via manipulations involving a series of URIs that is not entirely handled by a vector application, as exploited in conjunction with CVE-2008-2540. NOTE: this issue exists because of an insufficient fix for CVE-2005-2267.
CVE-2008-2934	Mozilla Firefox 3 before 3.0.1 on Mac OS X allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted GIF file that triggers a free of an uninitialized pointer.
CVE-2008-3198	Mozilla Firefox 3.x before 3.0.1 allows remote attackers to inject arbitrary web script into a chrome document via unspecified vectors, as demonstrated by injection into a XUL error page. NOTE: this can be leveraged to execute arbitrary code using CVE-2008-2933.
CVE-2008-3444	The content layout component in Mozilla Firefox 3.0 and 3.0.1 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted but well-formed web page that contains "a simple set of legitimate HTML tags."
CVE-2008-3836	feedWriter in Mozilla Firefox before 2.0.0.17 allows remote attackers to execute scripts with chrome privileges via vectors related to feed preview and the (1) elem.doCommand, (2) elem.dispatchEvent, (3) _setTitleText, (4) _setTitleImage, and (5) _initSubscriptionUI functions.
CVE-2008-3837	Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, and SeaMonkey before 1.1.12, allow user-assisted remote attackers to move a window during a mouse click, and possibly force a file download or unspecified other drag-and-drop action, via a crafted onmousedown action that calls window.moveBy, a variant of CVE-2003-0823.
CVE-2008-4059	The XPConnect component in Mozilla Firefox before 2.0.0.17 allows remote attackers to "pollute XPCNativeWrappers" and execute arbitrary code with chrome privileges via vectors related to a SCRIPT element.
CVE-2008-4063	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.2 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 (1) a zero value of the "this" variable in the nsContentList::Item function; (2) interaction of the indic IME extension, a Hindi language selection, and the "g" character; and (3) interaction of the nsFrameList::SortByContentOrder function with a certain insufficient protection of inline frames.
CVE-2008-4064	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to graphics rendering and (1) handling of a long alert messagebox in the cairo_surface_set_device_offset function, (2) integer overflows when handling animated PNG data in the info_callback function in nsPNGDecoder.cpp, and (3) an integer overflow when handling SVG data in the nsSVGFEGaussianBlurElement::SetupPredivide function in nsSVGFilters.cpp.
CVE-2008-4066	Mozilla Firefox 2.0.0.14, and other versions before 2.0.0.17, allows remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via HTML-escaped low surrogate characters that are ignored by the HTML parser, as demonstrated by a "jav&#56325ascript" sequence, aka "HTML escaped low surrogates bug."
CVE-2008-4069	The XBM decoder in Mozilla Firefox before 2.0.0.17 and SeaMonkey before 1.1.12 allows remote attackers to read uninitialized memory, and possibly obtain sensitive information in opportunistic circumstances, via a crafted XBM image file.
CVE-2008-4324	The user interface event dispatcher in Mozilla Firefox 3.0.3 on Windows XP SP2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a series of keypress, click, onkeydown, onkeyup, onmousedown, and onmouseup events. NOTE: it was later reported that Firefox 3.0.2 on Mac OS X 10.5 is also affected.
CVE-2008-4582	Mozilla Firefox 3.0.1 through 3.0.3, Firefox 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13, when running on Windows, do not properly identify the context of Windows .url shortcut files, which allows user-assisted remote attackers to bypass the Same Origin Policy and obtain sensitive information via an HTML document that is directly accessible through a filesystem, as demonstrated by documents in (1) local folders, (2) Windows share folders, and (3) RAR archives, and as demonstrated by IFRAMEs referencing shortcuts that point to (a) about:cache?device=memory and (b) about:cache?device=disk, a variant of CVE-2008-2810.
CVE-2008-4723	Multiple cross-site scripting (XSS) vulnerabilities in Mozilla Firefox 3.0.1 through 3.0.3 allow remote attackers to inject arbitrary web script or HTML via an ftp:// URL for an HTML document within a (1) JPG, (2) PDF, or (3) TXT file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2008-4821	Adobe Flash Player 9.0.124.0 and earlier, when a Mozilla browser is used, does not properly interpret jar: URLs, which allows attackers to obtain sensitive information via unknown vectors.

CVE-2008-5013	Mozilla Firefox 2.x before 2.0.0.18 and SeaMonkey 1.x before 1.1.13 do not properly check when the Flash module has been dynamically unloaded properly, which allows remote attackers to execute arbitrary code via a crafted SWF file that "dynamically unloads itself from an outside JavaScript function," which triggers an access of an expired memory address.
CVE-2008-5015	Mozilla Firefox 3.x before 3.0.4 assigns chrome privileges to a file: URI when it is accessed in the same tab from a chrome or privileged about: page, which makes it easier for user-assisted attackers to execute arbitrary JavaScript with chrome privileges via malicious code in a file that has already been saved on the local system.
CVE-2008-5019	The session restore feature in Mozilla Firefox 3.x before 3.0.4 and 2.x before 2.0.0.18 allows remote attackers to violate the same origin policy to conduct cross-site scripting (XSS) attacks and execute arbitrary JavaScript with chrome privileges via unknown vectors.
CVE-2008-5023	Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to bypass the protection mechanism for codebase principals and execute arbitrary script via the -moz-binding CSS property in a signed JAR file.
CVE-2008-5504	Mozilla Firefox 2.x before 2.0.0.19 allows remote attackers to run arbitrary JavaScript with chrome privileges via vectors related to the feed preview, a different vulnerability than CVE-2008-3836.
CVE-2008-5505	Mozilla Firefox 3.x before 3.0.5 allows remote attackers to bypass intended privacy restrictions by using the persist attribute in an XUL element to create and access data entities that are similar to cookies.
CVE-2008-5513	Unspecified vulnerability in the session-restore feature in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19 allows remote attackers to bypass the same origin policy, inject content into documents associated with other domains, and conduct cross-site scripting (XSS) attacks via unknown vectors related to restoration of SessionStore data.
CVE-2008-5697	The skype_tool.copy_num method in the Skype extension BETA 2.2.0.95 for Firefox allows remote attackers to write arbitrary data to the clipboard via a string argument.
CVE-2008-5715	Mozilla Firefox 3.0.5 on Windows Vista allows remote attackers to cause a denial of service (application crash) via JavaScript code with a long string value for the hash property (aka location.hash). NOTE: it was later reported that earlier versions are also affected, and that the impact is CPU consumption and application hang in unspecified circumstances perhaps involving other platforms.
CVE-2008-5822	Memory leak in Libxul, as used in Mozilla Firefox 3.0.5 and other products, allows remote attackers to cause a denial of service (memory consumption and browser hang) via a long CLASS attribute in an HR element in an HTML document.
CVE-2008-5913	The Math.random function in the JavaScript implementation in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, and SeaMonkey before 2.0.5, uses a random number generator that is seeded only once per browser session, which makes it easier for remote attackers to track a user, or trick a user into acting upon a spoofed pop-up message, by calculating the seed value, related to a "temporary footprint" and an "in-session phishing attack."
CVE-2008-7244	Mozilla Firefox 3.0.1 and earlier allows remote attackers to cause a denial of service (browser hang) by calling the window.print function in a loop, aka a "printing DoS attack," possibly a related issue to CVE-2009-0821.
CVE-2008-7293	Mozilla Firefox before 4 cannot properly restrict modifications to cookies established in HTTPS sessions, which allows man-in-the-middle attackers to overwrite or delete arbitrary cookies via a Set-Cookie header in an HTTP response, related to lack of the HTTP Strict Transport Security (HSTS) includeSubDomains feature, aka a "cookie forcing" issue.
CVE-2009-0068	Interaction error in xdg-open allows remote attackers to execute arbitrary code by sending a file with a dangerous MIME type but using a safe type that Firefox sends to xdg-open, which causes xdg-open to process the dangerous file type through automatic type detection, as demonstrated by overwriting the .desktop file.
CVE-2009-0071	Mozilla Firefox 3.0.5 and earlier 3.0.x versions, when designMode is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a certain (a) replaceChild or (b) removeChild call, followed by a (1) queryCommandValue, (2) queryCommandState, or (3) queryCommandIndeterm call. NOTE: it was later reported that 3.0.6 and 3.0.7 are also affected.
CVE-2009-0253	Mozilla Firefox 3.0.5 allows remote attackers to trick a user into visiting an arbitrary URL via an onclick action that moves a crafted element to the current mouse position, related to a "Status Bar Obfuscation" and "Clickjacking" attack.
CVE-2009-0354	Cross-domain vulnerability in js/src/jsobj.cpp in Mozilla Firefox 3.x before 3.0.6 allows remote attackers to bypass the Same Origin Policy, and access the properties of an arbitrary window and conduct cross-site scripting (XSS) attacks, via vectors involving a chrome XBL method and the window.eval function.
CVE-2009-0355	components/sessionstore/src/nsSessionStore.js in Mozilla Firefox before 3.0.6 does not block changes of INPUT elements to type="file" during tab restoration, which allows user-assisted remote attackers to read arbitrary files on a client machine via a crafted INPUT element.
CVE-2009-0356	Mozilla Firefox before 3.0.6 and SeaMonkey do not block links to the (1) about:plugins and (2) about:config URIs from .desktop files, which allows user-assisted remote attackers to bypass the Same Origin Policy and execute arbitrary code with chrome privileges via vectors involving the URL field in a Desktop Entry section of a .desktop file, related to representation of about: URIs as jar:file:// URIs. NOTE: this issue exists because of an incomplete fix for CVE-2008-4582.

CVE-2009-0357	Mozilla Firefox before 3.0.6 and SeaMonkey before 1.1.15 do not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls, related to the HTTPOnly protection mechanism.
CVE-2009-0358	Mozilla Firefox 3.x before 3.0.6 does not properly implement the (1) no-store and (2) no-cache Cache-Control directives, which allows local users to obtain sensitive information by using the (a) back button or (b) history list of the victim's browser, as demonstrated by reading the response page of an https POST request.
CVE-2009-0581	Memory leak in LittleCMS (aka lcms or liblcms) before 1.18beta2, as used in Firefox 3.1beta, OpenJDK, and GIMP, allows context-dependent attackers to cause a denial of service (memory consumption and application crash) via a crafted image file.
CVE-2009-0689	Array index error in the (1) dtoa implementation in dtoa.c (aka pdtoa.c) and the (2) gdtoa (aka new dtoa) implementation in gdtoa/misc.c in libc, as used in multiple operating systems and products including in FreeBSD 6.4 and 7.2, NetBSD 5.0, OpenBSD 4.5, Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4, K-Meleon 1.5.3, SeaMonkey 1.1.8, and other products, allows context-dependent attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a large precision value in the format argument to a printf function, which triggers incorrect memory allocation and a heap-based buffer overflow during conversion to a floating-point number.
CVE-2009-0723	Multiple integer overflows in LittleCMS (aka lcms or liblcms) before 1.18beta2, as used in Firefox 3.1beta, OpenJDK, and GIMP, allow context-dependent attackers to execute arbitrary code via a crafted image file that triggers a heap-based buffer overflow. NOTE: some of these details are obtained from third party information.
CVE-2009-0733	Multiple stack-based buffer overflows in the ReadSetOfCurves function in LittleCMS (aka lcms or liblcms) before 1.18beta2, as used in Firefox 3.1beta, OpenJDK, and GIMP, allow context-dependent attackers to execute arbitrary code via a crafted image file associated with a large integer value for the (1) input or (2) output channel, related to the ReadLUT_A2B and ReadLUT_B2A functions.
CVE-2009-0821	Mozilla Firefox 2.0.0.20 and earlier allows remote attackers to cause a denial of service (application crash) via nested calls to the window.print function, as demonstrated by a window.print(window.print()) in the onclick attribute of an INPUT element.
CVE-2009-1044	Mozilla Firefox 3.0.7 on Windows 7 allows remote attackers to execute arbitrary code via unknown vectors related to the _moveToEdgeShift XUL tree method, which triggers garbage collection on objects that are still in use, as demonstrated by Nils during a PWN2OWN competition at CanSecWest 2009.
CVE-2009-1169	The txMozillaXSLTProcessor::TransformToDoc function in Mozilla Firefox before 3.0.8 and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an XML file with a crafted XSLT transform.
CVE-2009-1232	Mozilla Firefox 3.0.8 and earlier 3.0.x versions allows remote attackers to cause a denial of service (memory corruption) via an XML document composed of a long series of start-tags with no corresponding end-tags. NOTE: it was later reported that 3.0.10 and earlier are also affected.
CVE-2009-1310	Cross-site scripting (XSS) vulnerability in the MozSearch plugin implementation in Mozilla Firefox before 3.0.9 allows user-assisted remote attackers to inject arbitrary web script or HTML via a javascript: URI in the SearchForm element.
CVE-2009-1311	Mozilla Firefox before 3.0.9 and SeaMonkey before 1.1.17 allow user-assisted remote attackers to obtain sensitive information via a web page with an embedded frame, which causes POST data from an outer page to be sent to the inner frame's URL during a SAVEMODE_FILEONLY save of the inner frame.
CVE-2009-1312	Mozilla Firefox before 3.0.9 and SeaMonkey 1.1.17 do not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header. NOTE: it was later reported that Firefox 3.6 a1 pre and Mozilla 1.7.x and earlier are also affected.
CVE-2009-1313	The nsTextFrame::ClearTextRun function in layout/generic/nsTextFrameThebes.cpp in Mozilla Firefox 3.0.9 allows remote attackers to cause a denial of service (memory corruption) and probably execute arbitrary code via unspecified vectors. NOTE: this vulnerability reportedly exists because of an incorrect fix for CVE-2009-1302.
CVE-2009-1571	Use-after-free vulnerability in the HTML parser 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 execute arbitrary code via unspecified method calls that attempt to access freed objects in low-memory situations.
CVE-2009-1597	Mozilla Firefox executes DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file, which might allow remote attackers to bypass intended Adobe Acrobat JavaScript restrictions on accessing the document object, as demonstrated by a web site that permits PDF uploads by untrusted users, and therefore has a shared document.domain between the web site and this javascript: URI. NOTE: the researcher reports that Adobe's position is "a PDF file is active content."
CVE-2009-1827	The SVG component in Mozilla Firefox 3.0.4 allows remote attackers to cause a denial of service (application hang) via a large value in the r (aka Radius) attribute of a circle element, related to an "unclamped loop."
CVE-2009-1828	Mozilla Firefox 3.0.10 allows remote attackers to cause a denial of service (infinite loop, application hang, and memory consumption) via a KEYGEN element in conjunction with (1) a META element specifying automatic page

	refresh or (2) a JavaScript onLoad event handler for a BODY element. NOTE: it was later reported that earlier versions are also affected.
CVE-2009-1834	Visual truncation vulnerability in netwerk/dns/src/nsIDNService.cpp in Mozilla Firefox before 3.0.11 and SeaMonkey before 1.1.17 allows remote attackers to spoof the location bar via an IDN with invalid Unicode characters that are displayed as whitespace, as demonstrated by the \u115A through \u115E characters.
CVE-2009-1835	Mozilla Firefox before 3.0.11 and SeaMonkey before 1.1.17 associate local documents with external domain names located after the file:// substring in a URL, which allows user-assisted remote attackers to read arbitrary cookies via a crafted HTML document, as demonstrated by a URL with file://example.com/C:/ at the beginning.
CVE-2009-1837	Race condition in the NPObjWrapper_NewResolve function in modules/plugin/base/src/nsJSNPRuntime.cpp in xul.dll in Mozilla Firefox 3 before 3.0.11 might allow remote attackers to execute arbitrary code via a page transition during Java applet loading, related to a use-after-free vulnerability for memory associated with a destroyed Java object.
CVE-2009-1839	Mozilla Firefox 3 before 3.0.11 associates an incorrect principal with a file: URL loaded through the location bar, which allows user-assisted remote attackers to bypass intended access restrictions and read files via a crafted HTML document, aka a "file-URL_to-file-URL scripting" attack.
CVE-2009-2011	Worldweaver DX Studio Player 3.0.29.0, 3.0.22.0, 3.0.12.0, and probably other versions before 3.0.29.1, when used as a plug-in for Firefox, does not restrict access to the shell.execute JavaScript API method, which allows remote attackers to execute arbitrary commands via a .dxstudio file that invokes this method.
CVE-2009-2043	nsViewManager.cpp in Mozilla Firefox 3.0.2 through 3.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors related to interaction with TinyMCE.
CVE-2009-2044	Mozilla Firefox 3.0.10 and earlier on Linux allows remote attackers to cause a denial of service (application crash) via a URI for a large GIF image in the BACKGROUND attribute of a BODY element.
CVE-2009-2061	Mozilla Firefox before 3.0.10 processes a 3xx HTTP CONNECT response before a successful SSL handshake, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying this CONNECT response to specify a 302 redirect to an arbitrary https web site.
CVE-2009-2065	Mozilla Firefox 3.0.10, and possibly other versions, detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable (HPIHSL) pages."
CVE-2009-2409	The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.
CVE-2009-2467	Mozilla Firefox before 3.0.12 and 3.5 before 3.5.1 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving a Flash object, a slow script dialog, and the unloading of the Flash plugin, which triggers attempted use of a deleted object.
CVE-2009-2468	Integer overflow in Apple CoreGraphics, as used in Safari before 4.0.3, Mozilla Firefox before 3.0.12, and Mac OS X 10.4.11 and 10.5.8, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long text run that triggers a heap-based buffer overflow during font glyph rendering, a related issue to CVE-2009-1194.
CVE-2009-2469	Mozilla Firefox before 3.0.12 does not properly handle an SVG element that has a property with a watch function and an __defineSetter__ function, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted document, related to a certain pointer misinterpretation.
CVE-2009-2470	Mozilla Firefox before 3.0.12, and 3.5.x before 3.5.2, allows remote SOCKS5 proxy servers to cause a denial of service (data stream corruption) via a long domain name in a reply.
CVE-2009-2471	The setTimeout function in Mozilla Firefox before 3.0.12 does not properly preserve object wrapping, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via a crafted call, related to XPCNativeWrapper.
CVE-2009-2472	Mozilla Firefox before 3.0.12 does not always use XPCCrossOriginWrapper when required during object construction, which allows remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via a crafted document, related to a "cross origin wrapper bypass."
CVE-2009-2477	js/src/jstracer.cpp in the Just-in-time (JIT) JavaScript compiler (aka TraceMonkey) in Mozilla Firefox 3.5 before 3.5.1 allows remote attackers to execute arbitrary code via certain use of the escape function that triggers access to uninitialized memory locations, as originally demonstrated by a document containing P and FONT elements.
CVE-2009-2478	Mozilla Firefox 3.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors, related to a "flash bug."
CVE-2009-2479	Mozilla Firefox 3.0.x, 3.5, and 3.5.1 on Windows allows remote attackers to cause a denial of service (uncaught exception and application crash) via a long Unicode string argument to the write method. NOTE: this was originally reported as a stack-based buffer overflow. NOTE: on Linux and Mac OS X, a crash resulting from this long string reportedly occurs in an operating-system library, not in Firefox.

CVE-2009-2654	Mozilla Firefox before 3.0.13, and 3.5.x before 3.5.2, allows remote attackers to spoof the address bar, and possibly conduct phishing attacks, via a crafted web page that calls window.open with an invalid character in the URL, makes document.write calls to the resulting object, and then calls the stop method during the loading of the error page.
CVE-2009-2662	The browser engine in Mozilla Firefox 3.5.x before 3.5.2 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the TraceRecorder::snapshot function in js/src/jstracer.cpp, and unspecified other vectors.
CVE-2009-2663	libvorbis before r16182, as used in Mozilla Firefox 3.5.x before 3.5.2 and other products, allows context-dependent attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted .ogg file.
CVE-2009-2664	The js_watch_set function in js/src/jsdbgapi.cpp in the JavaScript engine in Mozilla Firefox before 3.0.12 allows remote attackers to cause a denial of service (assertion failure and application exit) or possibly execute arbitrary code via a crafted .js file, related to a "memory safety bug." NOTE: this was originally reported as affecting versions before 3.0.13.
CVE-2009-2665	The nsDocument::SetScriptGlobalObject function in content/base/src/nsDocument.cpp in Mozilla Firefox 3.5.x before 3.5.2, when certain add-ons are enabled, does not properly handle a Link HTTP header, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via a crafted web page, related to an incorrect security wrapper.
CVE-2009-2953	Mozilla Firefox 3.0.6 through 3.0.13, and 3.5.x, allows remote attackers to cause a denial of service (CPU consumption) via JavaScript code with a long string value for the hash property (aka location.hash), a related issue to CVE-2008-5715.
CVE-2009-2975	Mozilla Firefox 3.5.2 on Windows XP, in some situations possibly involving an incompletely configured protocol handler, does not properly implement setting the document.location property to a value specifying a protocol associated with an external application, which allows remote attackers to cause a denial of service (memory consumption) via vectors involving a series of function calls that set this property, as demonstrated by (1) the chromehtml: protocol and (2) the aim: protocol.
CVE-2009-3007	Mozilla Firefox 3.5.1 and SeaMonkey 1.1.17, and Flock 2.5.1, allow context-dependent attackers to spoof the address bar, via window.open with a relative URI, to show an arbitrary file: URL after a victim has visited any file: URL, as demonstrated by a visit to a file: document written by the attacker.
CVE-2009-3010	Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: in some product versions, the JavaScript executes outside of the context of the HTTP site.
CVE-2009-3012	Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre does not properly block data: URIs in Location headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Location header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Location header. NOTE: the JavaScript executes outside of the context of the HTTP site.
CVE-2009-3014	Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly handle javascript: URIs in HTML links within 302 error documents sent from web servers, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Location HTTP response header or (2) specifying the content of a Location HTTP response header.
CVE-2009-3069	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3070	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3071	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.2, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3072	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.14 and 3.5.x before 3.5.3, 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 vectors related to the BinHex decoder in netwerk/streamconv/converter/nsBinHexDecoder.cpp, and unknown vectors.
CVE-2009-3073	Unspecified vulnerability in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

CVE-2009-3074	Unspecified vulnerability in the JavaScript engine in Mozilla Firefox before 3.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3075	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox before 3.0.14 and 3.5.x before 3.5.2, 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 vectors related to use of mutable strings in the <code>js_StringReplaceHelper</code> function in <code>js/src/jsstr.cpp</code> , and unknown vectors.
CVE-2009-3076	Mozilla Firefox before 3.0.14 does not properly implement certain dialogs associated with the (1) <code>pkcs11.addmodule</code> and (2) <code>pkcs11.deletemodule</code> operations, which makes it easier for remote attackers to trick a user into installing or removing an arbitrary PKCS11 module.
CVE-2009-3077	Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.3, does not properly manage pointers for the columns (aka <code>TreeColumns</code> ) of a XUL tree element, which allows remote attackers to execute arbitrary code via a crafted HTML document, related to a "dangling pointer vulnerability."
CVE-2009-3078	Visual truncation vulnerability in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.3, allows remote attackers to trigger a vertical scroll and spoof URLs via unspecified Unicode characters with a tall line-height property.
CVE-2009-3079	Unspecified vulnerability in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.3, allows remote attackers to execute arbitrary JavaScript with chrome privileges via vectors involving an object, the <code>FeedWriter</code> , and the <code>BrowserFeedWriter</code> .
CVE-2009-3274	Mozilla Firefox 3.6a1, 3.5.3, 3.5.2, and earlier 3.5.x versions, and 3.0.14 and earlier 2.x and 3.x versions, on Linux uses a predictable <code>/tmp</code> pathname for files selected from the Downloads window, which allows local users to replace an arbitrary downloaded file by placing a file in a <code>/tmp</code> location before the download occurs, related to the Download Manager component. NOTE: some of these details are obtained from third party information.
CVE-2009-3370	Mozilla Firefox before 3.0.15, and 3.5.x before 3.5.4, allows remote attackers to read form history by forging mouse and keyboard events that leverage the auto-fill feature to populate form fields, in an attacker-readable form, with history entries.
CVE-2009-3371	Use-after-free vulnerability in Mozilla Firefox 3.5.x before 3.5.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by creating JavaScript web-workers recursively.
CVE-2009-3372	Mozilla Firefox before 3.0.15 and 3.5.x before 3.5.4, and SeaMonkey before 2.0, allows remote attackers to execute arbitrary code via a crafted regular expression in a Proxy Auto-configuration (PAC) file.
CVE-2009-3373	Heap-based buffer overflow in the GIF image parser in Mozilla Firefox before 3.0.15 and 3.5.x before 3.5.4, and SeaMonkey before 2.0, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2009-3374	The <code>XPCVariant::VariantDataToJS</code> function in the XPCOM implementation in Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4 does not enforce intended restrictions on interaction between chrome privileged code and objects obtained from remote web sites, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via unspecified method calls, related to "doubly-wrapped objects."
CVE-2009-3375	content/html/document/src/nsHTMLDocument.cpp in Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4 allows user-assisted remote attackers to bypass the Same Origin Policy and read an arbitrary content selection via the <code>document.getSelection</code> function.
CVE-2009-3376	Mozilla Firefox before 3.0.15 and 3.5.x before 3.5.4, and SeaMonkey before 2.0, does not properly handle a right-to-left override (aka RLO or U+202E) Unicode character in a download filename, which allows remote attackers to spoof file extensions via a crafted filename, as demonstrated by displaying a non-executable extension for an executable file.
CVE-2009-3377	Multiple unspecified vulnerabilities in liboggz before cf5feeab69b05e24, as used in Mozilla Firefox 3.5.x before 3.5.4, allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3378	The <code>oggplay_data_handle_theora_frame</code> function in <code>media/liboggplay/src/liboggplay/oggplay_data.c</code> in liboggplay, as used in Mozilla Firefox 3.5.x before 3.5.4, attempts to reuse an earlier frame data structure upon encountering a decoding error for the first frame, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via a crafted .ogg video file.
CVE-2009-3379	Multiple unspecified vulnerabilities in libvorbis, as used in Mozilla Firefox 3.5.x before 3.5.4, allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors. NOTE: this might overlap CVE-2009-2663.
CVE-2009-3380	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3381	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3382	<code>layout/base/nsCSSFrameConstructor.cpp</code> in the browser engine in Mozilla Firefox 3.0.x before 3.0.15 does not properly handle first-letter frames, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.

CVE-2009-3383	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3388	liboggplay in Mozilla Firefox 3.5.x before 3.5.6 and SeaMonkey before 2.0.1 might allow context-dependent attackers to cause a denial of service (application crash) or execute arbitrary code via unspecified vectors, related to "memory safety issues."
CVE-2009-3389	Integer overflow in libtheora in Xiph.Org Theora before 1.1, as used in Mozilla Firefox 3.5 before 3.5.6 and SeaMonkey before 2.0.1, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a video with large dimensions.
CVE-2009-3478	Argument injection vulnerability in (1) src/content/js/connection/sftp.js and (2) src/content/js/connection/controlSocket.js.in in FireFTP Extension 1.0.5 for Firefox allows remote authenticated SFTP users to cause victims to alter permissions, delete, download, or move the wrong file via a filename containing " (double quotes), which is not properly filtered or encoded when FireFTP constructs the command to send to psftp.exe.
CVE-2009-3978	The nsGIFDecoder2::GifWrite function in decoders/gif/nsGIFDecoder2.cpp in libpr0n in Mozilla Firefox before 3.5.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an animated GIF file with a large image size, a different vulnerability than CVE-2009-3373.
CVE-2009-3979	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.16 and 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-2009-3985	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to associate spoofed content with an invalid URL by setting document.location to this URL, and then writing arbitrary web script or HTML to the associated blank document, a related issue to CVE-2009-2654.
CVE-2009-3986	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to execute arbitrary JavaScript with chrome privileges by leveraging a reference to a chrome window from a content window, related to the window.opener property.
CVE-2009-3987	The GeckoActiveXObject function in Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, generates different exception messages depending on whether the referenced COM object is listed in the registry, which allows remote attackers to obtain potentially sensitive information about installed software by making multiple calls that specify the ProgID values of different COM objects.
CVE-2009-3988	Mozilla Firefox 3.0.x before 3.0.18 and 3.5.x before 3.5.8, and SeaMonkey before 2.0.3, does not properly restrict read access to object properties in showModalDialog, which allows remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via crafted dialogArguments values.
CVE-2009-4100	Yoono extension before 6.1.1 for Firefox performs certain operations with chrome privileges, which allows user-assisted remote attackers to execute arbitrary commands and perform cross-domain scripting attacks via DOM event handlers such as onload.
CVE-2009-4101	infoRSS 1.1.4.2 and earlier extension for Firefox performs certain operations with chrome privileges, which allows remote attackers to execute arbitrary commands and perform cross-domain scripting attacks via the description tag of an RSS feed.
CVE-2009-4102	Sage 1.4.3 and earlier extension for Firefox performs certain operations with chrome privileges, which allows remote attackers to execute arbitrary commands and perform cross-domain scripting attacks via the description tag of an RSS feed.
CVE-2009-4127	Unspecified vulnerability in Wikipedia Toolbar extension before 0.5.9.2 for Firefox allows user-assisted remote attackers to execute arbitrary JavaScript with Chrome privileges via vectors involving unspecified Toolbar buttons and the eval function. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2009-4129	Race condition in Mozilla Firefox allows remote attackers to produce a JavaScript message with a spoofed domain association by writing the message in between the document request and document load for a web page in a different domain.
CVE-2009-4130	Visual truncation vulnerability in the MakeScriptDialogTitle function in nsGlobalWindow.cpp in Mozilla Firefox allows remote attackers to spoof the origin domain name of a script via a long name.
CVE-2009-5017	Mozilla Firefox before 3.6 Beta 3 does not properly handle overlong UTF-8 encoding, which makes it easier for remote attackers to bypass cross-site scripting (XSS) protection mechanisms via a crafted string, a different vulnerability than CVE-2010-1210.
CVE-2010-0160	The Web Worker functionality in Mozilla Firefox 3.0.x before 3.0.18 and 3.5.x before 3.5.8, and SeaMonkey before 2.0.3, does not properly handle array data types for posted messages, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2010-0162	Mozilla Firefox 3.0.x before 3.0.18 and 3.5.x before 3.5.8, and SeaMonkey before 2.0.3, does not properly support the application/octet-stream content type as a protection mechanism against execution of web script in certain

	circumstances involving SVG and the EMBED element, which allows remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via an embedded SVG document.
CVE-2010-0164	Use-after-free vulnerability in the imgContainer::InternalAddFrameHelper function in src/imgContainer.cpp in libpr0n in Mozilla Firefox 3.6 before 3.6.2 allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a multipart/x-mixed-replace animation in which the frames have different bits-per-pixel (bpp) values.
CVE-2010-0165	The TraceRecorder::traverseScopeChain function in js/src/jstracer.cpp in the browser engine in Mozilla Firefox 3.6 before 3.6.2 allows remote attackers to cause a denial of service (memory corruption and application crash) and possibly execute arbitrary code via vectors involving certain indirect calls to the JavaScript eval function.
CVE-2010-0166	The gfxTextRun::SanitizeGlyphRuns function in gfx/thebes/src/gfxFont.cpp in the browser engine in Mozilla Firefox 3.6 before 3.6.2 on Mac OS X, when the Core Text API is used, does not properly perform certain deletions, which allows remote attackers to cause a denial of service (memory corruption and application crash) and possibly execute arbitrary code via an HTML document containing invisible Unicode characters, as demonstrated by the U+FEFF, U+FFF9, U+FFFA, and U+FFFB characters.
CVE-2010-0168	The nsDocument::MaybePreLoadImage function in content/base/src/nsDocument.cpp in the image-preloading implementation in Mozilla Firefox 3.6 before 3.6.2 does not apply scheme restrictions and policy restrictions to the image's URL, which might allow remote attackers to cause a denial of service (application crash or hang) or hijack the functionality of the browser's add-ons via a crafted SRC attribute of an IMG element, as demonstrated by remote command execution through an ssh: URL in a configuration that supports gnome-vfs with a nonstandard network.gnomevfs.supported-protocols setting.
CVE-2010-0170	Mozilla Firefox 3.6 before 3.6.2 does not offer plugins the expected window.location protection mechanism, which might allow remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via vectors that are specific to each affected plugin.
CVE-2010-0172	toolkit/components/passwordmgr/src/nsLoginManagerPrompter.js in the asynchronous Authorization Prompt implementation in Mozilla Firefox 3.6 before 3.6.2 does not properly handle concurrent authorization requests from multiple web sites, which might allow remote web servers to spoof an authorization dialog and capture credentials by demanding HTTP authentication in opportunistic circumstances.
CVE-2010-0177	Mozilla Firefox before 3.0.19, 3.5.x before 3.5.9, and 3.6.x before 3.6.2, and SeaMonkey before 2.0.4, frees the contents of the window.navigator.plugins array while a reference to an array element is still active, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to a "dangling pointer vulnerability."
CVE-2010-0178	Mozilla Firefox before 3.0.19, 3.5.x before 3.5.9, and 3.6.x before 3.6.2, and SeaMonkey before 2.0.4, does not prevent applets from interpreting mouse clicks as drag-and-drop actions, which allows remote attackers to execute arbitrary JavaScript with Chrome privileges by loading a chrome: URL and then loading a javascript: URL.
CVE-2010-0181	Mozilla Firefox before 3.5.9 and 3.6.x before 3.6.2, and SeaMonkey before 2.0.4, executes a mail application in situations where an IMG element has a SRC attribute that is a redirect to a mailto: URL, which allows remote attackers to cause a denial of service (excessive application launches) via an HTML document with many images.
CVE-2010-0183	Use-after-free vulnerability in the nsCycleCollector::MarkRoots function in Mozilla Firefox 3.5.x before 3.5.10 and SeaMonkey before 2.0.5 allows remote attackers to execute arbitrary code via a crafted HTML document, related to an improper frame construction process for menus.
CVE-2010-0220	The nsObserverList::FillObserverArray function in xpcom/ds/nsObserverList.cpp in Mozilla Firefox before 3.5.7 allows remote attackers to cause a denial of service (application crash) via a crafted web site that triggers memory consumption and an accompanying Low Memory alert dialog, and also triggers attempted removal of an observer from an empty observers array.
CVE-2010-0648	Mozilla Firefox, possibly before 3.6, allows remote attackers to discover a redirect's target URL, for the session of a specific user of a web site, by placing the site's URL in the HREF attribute of a stylesheet LINK element, and then reading the document.styleSheets[0].href property value, related to an IFRAME element.
CVE-2010-1028	Integer overflow in the decompression functionality in the Web Open Fonts Format (WOFF) decoder in Mozilla Firefox 3.6 before 3.6.2 and 3.7 before 3.7 alpha 3 allows remote attackers to execute arbitrary code via a crafted WOFF file that triggers a buffer overflow, as demonstrated by the vd_ff module in VulnDisco 9.0.
CVE-2010-1121	Mozilla Firefox 3.6.x before 3.6.3 does not properly manage the scopes of DOM nodes that are moved from one document to another, which allows remote attackers to conduct use-after-free attacks and execute arbitrary code via unspecified vectors involving improper interaction with garbage collection, as demonstrated by Nils during a Pwn2Own competition at CanSecWest 2010.
CVE-2010-1122	Unspecified vulnerability in Mozilla Firefox 3.5.x through 3.5.8 allows remote attackers to cause a denial of service (memory corruption and application crash) and possibly have unknown other impact via vectors that might involve compressed data, a different vulnerability than CVE-2010-1028.
CVE-2010-1125	The JavaScript implementation in Mozilla Firefox 3.x before 3.5.10 and 3.6.x before 3.6.4, and SeaMonkey before 2.0.5, allows remote attackers to send selected keystrokes to a form field in a hidden frame, instead of the intended form field in a visible frame, via certain calls to the focus method.

CVE-2010-1197	Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, and SeaMonkey before 2.0.5, does not properly handle situations in which both "Content-Disposition: attachment" and "Content-Type: multipart" are present in HTTP headers, which allows remote attackers to conduct cross-site scripting (XSS) attacks via an uploaded HTML document.
CVE-2010-1198	Use-after-free vulnerability in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, and SeaMonkey before 2.0.5, allows remote attackers to execute arbitrary code via vectors involving multiple plugin instances.
CVE-2010-1203	The JavaScript engine in Mozilla Firefox 3.6.x before 3.6.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors that trigger an assertion failure in jstracer.cpp.
CVE-2010-1206	The startDocumentLoad function in browser/base/content/browser.js in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, does not properly implement the Same Origin Policy in certain circumstances related to the about:blank document and a document that is currently loading, which allows (1) remote web servers to conduct spoofing attacks via vectors involving a 204 (aka No Content) status code, and allows (2) remote attackers to conduct spoofing attacks via vectors involving a window.stop call.
CVE-2010-1208	Use-after-free vulnerability in the attribute-cloning functionality in the DOM implementation in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, allows remote attackers to execute arbitrary code via vectors related to deletion of an event attribute node with a nonzero reference count.
CVE-2010-1209	Use-after-free vulnerability in the NodeIterator implementation in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, allows remote attackers to execute arbitrary code via a crafted NodeFilter that detaches DOM nodes, related to the NodeIterator interface and a javascript callback.
CVE-2010-1214	Integer overflow in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, allows remote attackers to execute arbitrary code via plugin content with many parameter elements.
CVE-2010-1986	Mozilla Firefox 3.6.3 on Windows XP SP3 allows remote attackers to cause a denial of service (memory consumption and application crash) via JavaScript code that creates multiple arrays containing elements with long string values, and then appends long strings to the content of a P element, related to the gfxWindowsFontGroup::MakeTextRun function in xul.dll, a different vulnerability than CVE-2009-1571.
CVE-2010-1987	Mozilla Firefox 3.6.3 on Windows XP SP3 allows remote attackers to cause a denial of service (memory consumption, out-of-bounds read, and application crash) via JavaScript code that appends long strings to the content of a P element, and performs certain other string concatenation and substring operations, related to the DoubleWideCharMappedString class in USP10.dll and the gfxWindowsFontGroup::GetUnderlineOffset function in xul.dll, a different vulnerability than CVE-2009-1571.
CVE-2010-1988	Mozilla Firefox 3.6.3 on Windows XP SP3 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via JavaScript code that performs certain string concatenation and substring operations, a different vulnerability than CVE-2009-1571.
CVE-2010-1990	Mozilla Firefox 3.6.x, 3.5.x, 3.0.19, and earlier, and SeaMonkey, executes a mail application in situations where an IFRAME element has a mailto: URL in its SRC attribute, which allows remote attackers to cause a denial of service (excessive application launches) via an HTML document with many IFRAME elements.
CVE-2010-2117	Mozilla Firefox 3.0.19, 3.5.x, and 3.6.x allows remote attackers to cause a denial of service (resource consumption) via JavaScript code containing an infinite loop that creates IFRAME elements for invalid (1) news:// or (2) nntp:// URIs.
CVE-2010-2751	The nsDocShell::OnRedirectStateChange function in docshell/base/nsDocShell.cpp in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, allows remote attackers to spoof the SSL security status of a document via vectors involving multiple requests, a redirect, and the history.back and history.forward JavaScript functions.
CVE-2010-2755	layout/generic/nsObjectFrame.cpp in Mozilla Firefox 3.6.7 does not properly free memory in the parameter array of a plugin instance, which allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted HTML document, related to the DATA and SRC attributes of an OBJECT element. NOTE: this vulnerability exists because of an incorrect fix for CVE-2010-1214.
CVE-2010-2792	Race condition in the SPICE (aka spice-xpi) plug-in 2.2 for Firefox allows local users to obtain sensitive information, and conduct man-in-the-middle attacks, by providing a UNIX socket for communication between this plug-in and the client (aka qspice-client) in qspice 0.3.0, and then accessing this socket.
CVE-2010-2794	The SPICE (aka spice-xpi) plug-in 2.2 for Firefox allows local users to overwrite arbitrary files via a symlink attack on an unspecified log file.
CVE-2010-3171	The Math.random function in the JavaScript implementation in Mozilla Firefox 3.5.10 through 3.5.11, 3.6.4 through 3.6.8, and 4.0 Beta1 uses a random number generator that is seeded only once per document object, which makes it easier for remote attackers to track a user, or trick a user into acting upon a spoofed pop-up message, by calculating the seed value, related to a "temporary footprint" and an "in-session phishing attack." NOTE: this vulnerability exists because of an incorrect fix for CVE-2008-5913.
CVE-2010-3177	Multiple cross-site scripting (XSS) vulnerabilities in the Gopher parser in Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, and SeaMonkey before 2.0.9, allow remote attackers to inject arbitrary web script or HTML via a crafted name of a (1) file or (2) directory on a Gopher server.

CVE-2010-3399	The <code>js_InitRandom</code> function in the JavaScript implementation in Mozilla Firefox 3.5.10 through 3.5.11, 3.6.4 through 3.6.8, and 4.0 Beta1 uses a context pointer in conjunction with its successor pointer for seeding of a random number generator, which makes it easier for remote attackers to guess the seed value via a brute-force attack, a different vulnerability than CVE-2010-3171.
CVE-2010-3400	The <code>js_InitRandom</code> function in the JavaScript implementation in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, and SeaMonkey before 2.0.5, uses the current time for seeding of a random number generator, which makes it easier for remote attackers to guess the seed value via a brute-force attack, a different vulnerability than CVE-2008-5913.
CVE-2010-3766	Use-after-free vulnerability in Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, allows remote attackers to execute arbitrary code via vectors involving a change to an <code>nsDOMAttribute</code> node.
CVE-2010-3767	Integer overflow in the <code>NewIdArray</code> function in Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, allows remote attackers to execute arbitrary code via a JavaScript array with many elements.
CVE-2010-3770	Multiple cross-site scripting (XSS) vulnerabilities in the rendering engine in Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, allow remote attackers to inject arbitrary web script or HTML via (1) x-mac-arabic, (2) x-mac-farsi, or (3) x-mac-hebrew characters that may be converted to angle brackets during rendering.
CVE-2010-3771	Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, does not properly handle injection of an <code>ISINDEX</code> element into an <code>about:blank</code> page, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges via vectors related to redirection to a chrome: URI.
CVE-2010-3772	Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, does not properly calculate index values for certain child content in a XUL tree, which allows remote attackers to execute arbitrary code via vectors involving a <code>DIV</code> element within a <code>treechildren</code> element.
CVE-2010-3773	Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, when the <code>XMLHttpRequestSpy</code> module in the Firebug add-on is used, does not properly handle interaction between the <code>XMLHttpRequestSpy</code> object and chrome privileged objects, which allows remote attackers to execute arbitrary JavaScript via a crafted HTTP response. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-0179.
CVE-2010-3774	The <code>NS_SecurityCompareURIs</code> function in <code>netwerk/base/public/nsNetUtil.h</code> in Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, does not properly handle (1) <code>about:nerror</code> and (2) <code>about:certerror</code> pages, which allows remote attackers to spoof the location bar via a crafted web site.
CVE-2010-3775	Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, and SeaMonkey before 2.0.11, does not properly handle certain redirections involving data: URLs and Java LiveConnect scripts, which allows remote attackers to start processes, read arbitrary local files, and establish network connections via vectors involving a refresh value in the <code>http-equiv</code> attribute of a <code>META</code> element, which causes the wrong security principal to be used.
CVE-2010-4508	The WebSockets implementation in Mozilla Firefox 4 through 4.0 Beta 7 does not properly perform proxy upgrade negotiation, which has unspecified impact and remote attack vectors, related to an "inherent problem" with the WebSocket specification.
CVE-2011-0012	The SPICE Firefox plug-in ( <code>spice-xpi</code> ) 2.4, 2.3, 2.2, and possibly other versions allows local users to overwrite arbitrary files via a symlink attack on the <code>usbrdrcrt</code> log file, which has a predictable name.
CVE-2011-0051	Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, and SeaMonkey before 2.0.12, does not properly handle certain recursive eval calls, which makes it easier for remote attackers to force a user to respond positively to a dialog question, as demonstrated by a question about granting privileges.
CVE-2011-0054	Buffer overflow in the JavaScript engine in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, and SeaMonkey before 2.0.12, might allow remote attackers to execute arbitrary code via vectors involving non-local JavaScript variables, aka an "upvarMap" issue.
CVE-2011-0055	Use-after-free vulnerability in the <code>JSON.stringify</code> method in <code>js3250.dll</code> in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, and SeaMonkey before 2.0.12, might allow remote attackers to execute arbitrary code via unspecified vectors related to the <code>js_HasOwnProperty</code> function and garbage collection.
CVE-2011-0056	Buffer overflow in the JavaScript engine in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, and SeaMonkey before 2.0.12, might allow remote attackers to execute arbitrary code via vectors involving exception timing and a large number of string values, aka an "atom map" issue.
CVE-2011-0057	Use-after-free vulnerability in the Web Workers implementation in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, and SeaMonkey before 2.0.12, allows remote attackers to execute arbitrary code via vectors related to a JavaScript Worker and garbage collection.
CVE-2011-0058	Buffer overflow in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, and SeaMonkey before 2.0.12, on Windows allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a long string that triggers construction of a long text run.
CVE-2011-0059	Cross-site request forgery (CSRF) vulnerability in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, and SeaMonkey before 2.0.12, allows remote attackers to hijack the authentication of arbitrary users for requests that were initiated by a plugin and received a 307 redirect to a page on a different web site.

CVE-2011-0064	The hb_buffer_ensure function in hb-buffer.c in HarfBuzz, as used in Pango 1.28.3, Firefox, and other products, does not verify that memory reallocations succeed, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via crafted OpenType font data that triggers use of an incorrect index.
CVE-2011-0065	Use-after-free vulnerability in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, allows remote attackers to execute arbitrary code via vectors related to OBJECT's mChannel.
CVE-2011-0066	Use-after-free vulnerability in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, allows remote attackers to execute arbitrary code via vectors related to OBJECT's mObserverList.
CVE-2011-0067	Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, does not properly implement autocompletion for forms, which allows remote attackers to read form history entries via a Java applet that spoofs interaction with the autocomplete controls.
CVE-2011-0073	Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, does not properly use nsTreeRange data structures, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to a "dangling pointer."
CVE-2011-0076	Unspecified vulnerability in the Java Embedding Plugin (JEP) in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, on Mac OS X allows remote attackers to bypass intended access restrictions via unknown vectors.
CVE-2011-0079	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x before 4.0.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to gfx/layers/d3d10/ReadbackManagerD3D10.cpp and unknown other vectors.
CVE-2011-0082	The X.509 certificate validation functionality in Mozilla Firefox 4.0.x through 4.0.1 does not properly implement single-session security exceptions, which might make it easier for user-assisted remote attackers to spoof an SSL server via an untrusted certificate that triggers potentially unwanted local caching of documents from that server.
CVE-2011-0341	Stack-based buffer overflow in the pdfmoz_onmouse function in apps/mozilla/moz_main.c in the MuPDF plug-in 2008.09.02 for Firefox allows remote attackers to execute arbitrary code via a crafted web site.
CVE-2011-1179	The SPICE Firefox plug-in (spice-xpi) 2.4, 2.3, 2.2, and possibly other versions allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to (1) plugin/nsScriptablePeer.cpp and (2) plugin/plugin.cpp, which trigger multiple uses of an uninitialized pointer.
CVE-2011-1712	The txXPathNodeUtils::getXSLTId function in txMozillaXPathTreeWalker.cpp and txStandaloneXPathTreeWalker.cpp in Mozilla Firefox before 3.5.19, 3.6.x before 3.6.17, and 4.x before 4.0.1, and SeaMonkey before 2.0.14, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function.
CVE-2011-2367	The WebGL implementation in Mozilla Firefox 4.x through 4.0.1 does not properly restrict read operations, which allows remote attackers to obtain sensitive information from GPU memory associated with an arbitrary process, or cause a denial of service (application crash), via unspecified vectors.
CVE-2011-2368	The WebGL implementation in Mozilla Firefox 4.x through 4.0.1 does not properly restrict write operations, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.
CVE-2011-2369	Cross-site scripting (XSS) vulnerability in Mozilla Firefox 4.x through 4.0.1 allows remote attackers to inject arbitrary web script or HTML via an SVG element containing an HTML-encoded entity.
CVE-2011-2370	Mozilla Firefox before 5.0 does not properly enforce the whitelist for the xpinstall functionality, which allows remote attackers to trigger an installation dialog for a (1) add-on or (2) theme via unspecified vectors.
CVE-2011-2598	The WebGL implementation in Mozilla Firefox 4.x allows remote attackers to obtain screenshots of the windows of arbitrary desktop applications via vectors involving an SVG filter, an IFRAME element, and uninitialized data in graphics memory.
CVE-2011-2740	EMC RSA Key Manager (RKM) Appliance 2.7 SP1 before 2.7.1.6, when Firefox 4.x or 5.0 is used, does not properly terminate a user session upon a logout action, which makes it easier for remote attackers to execute arbitrary code by leveraging an unattended workstation.
CVE-2011-2990	The implementation of Content Security Policy (CSP) violation reports in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3, and possibly other products does not remove proxy-authorization credentials from the listed request headers, which allows attackers to obtain sensitive information by reading a report, related to incorrect host resolution that occurs with certain redirects.
CVE-2011-2993	The implementation of digital signatures for JAR files in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3, and possibly other products does not prevent calls from unsigned JavaScript code to signed code, which allows remote attackers to bypass the Same Origin Policy and gain privileges via a crafted web site, a different vulnerability than CVE-2008-2801.
CVE-2011-2996	Unspecified vulnerability in the plugin API in Mozilla Firefox 3.6.x before 3.6.23 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-2998	Integer underflow in Mozilla Firefox 3.6.x before 3.6.23 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via JavaScript code containing a large RegExp expression.

CVE-2011-3002	Almost Native Graphics Layer Engine (ANGLE), as used in Mozilla Firefox before 7.0 and SeaMonkey before 2.4, does not validate the return value of a GrowAtomTable function call, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger a memory-allocation error and a resulting buffer overflow.
CVE-2011-3003	Mozilla Firefox before 7.0 and SeaMonkey before 2.4 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unspecified WebGL test case that triggers a memory-allocation error and a resulting out-of-bounds write operation.
CVE-2011-3004	The JSSubScriptLoader in Mozilla Firefox 4.x through 6 and SeaMonkey before 2.4 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.
CVE-2011-3339	Cross-site scripting (XSS) vulnerability in the Admin Control Center in Sentinel HASP Run-time Environment 5.95 and earlier in SafeNet Sentinel HASP (formerly Aladdin HASP SRM) run-time installer before 6.x and SDK before 5.11, as used in 7 Technologies (7T) IGSS 7 and other products, when Firefox 2.0 is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors that trigger write access to a configuration file.
CVE-2011-3384	Cross-site scripting (XSS) vulnerability in the Sage add-on 1.3.10 and earlier for Firefox allows remote attackers to inject arbitrary web script or HTML via a crafted feed, a different vulnerability than CVE-2009-4102.
CVE-2011-3866	Mozilla Firefox before 7.0 and SeaMonkey before 2.4 do not properly restrict availability of motion data events, which makes it easier for remote attackers to read keystrokes by leveraging JavaScript code running in a background tab.
CVE-2011-4688	Mozilla Firefox 8.0.1 and earlier does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.
CVE-2012-0450	Mozilla Firefox 4.x through 9.0 and SeaMonkey before 2.7 on Linux and Mac OS X set weak permissions for Firefox Recovery Key.html, which might allow local users to read a Firefox Sync key via standard filesystem operations.
CVE-2012-1950	The drag-and-drop implementation in Mozilla Firefox 4.x through 13.0 and Firefox ESR 10.x before 10.0.6 allows remote attackers to spoof the address bar by canceling a page load.
CVE-2012-1965	Mozilla Firefox 4.x through 13.0 and Firefox ESR 10.x before 10.0.6 do not properly establish the security context of a feed: URL, which allows remote attackers to bypass unspecified cross-site scripting (XSS) protection mechanisms via a feed:javascript: URL.
CVE-2012-1966	Mozilla Firefox 4.x through 13.0 and Firefox ESR 10.x before 10.0.6 do not have the same context-menu restrictions for data: URLs as for javascript: URLs, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted URL.
CVE-2012-3965	Mozilla Firefox before 15.0 does not properly restrict navigation to the about:newtab page, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges via a crafted web site that triggers creation of a new tab and then a new window.
CVE-2012-3973	The debugger in the developer-tools subsystem in Mozilla Firefox before 15.0, when remote debugging is disabled, does not properly restrict access to the remote-debugging service, which allows remote attackers to execute arbitrary code by leveraging the presence of the HTTPMonitor extension and connecting to that service through the HTTPMonitor port.
CVE-2012-3979	Mozilla Firefox before 15.0 on Android does not properly implement unspecified callers of the __android_log_print function, which allows remote attackers to execute arbitrary code via a crafted web page that calls the JavaScript dump function.
CVE-2012-3987	Mozilla Firefox before 16.0 on Android assigns chrome privileges to Reader Mode pages, which allows user-assisted remote attackers to bypass intended access restrictions via a crafted web site.
CVE-2012-4190	The FT2FontEntry::CreateFontEntry function in FreeType, as used in the Android build of Mozilla Firefox before 16.0.1 on CyanogenMod 10, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2012-4203	The New Tab page in Mozilla Firefox before 17.0 uses a privileged context for execution of JavaScript code by bookmarklets, which allows user-assisted remote attackers to run arbitrary programs by leveraging a javascript: URL in a bookmark.
CVE-2012-4206	Untrusted search path vulnerability in the installer in Mozilla Firefox before 17.0 and Firefox ESR 10.x before 10.0.11 on Windows allows local users to gain privileges via a Trojan horse DLL in the default downloads directory.
CVE-2012-4210	The Style Inspector in Mozilla Firefox before 17.0 and Firefox ESR 10.x before 10.0.11 does not properly restrict the context of HTML markup and Cascading Style Sheets (CSS) token sequences, which allows user-assisted remote attackers to execute arbitrary JavaScript code with chrome privileges via a crafted stylesheet.
CVE-2012-5837	The Web Developer Toolbar in Mozilla Firefox before 17.0 executes script with chrome privileges, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via a crafted string.

CVE-2013-0751	Mozilla Firefox before 18.0 on Android and SeaMonkey before 2.15 do not restrict a touch event to a single IFRAME element, which allows remote attackers to obtain sensitive information or possibly conduct cross-site scripting (XSS) attacks via a crafted HTML document.
CVE-2013-0789	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 20.0 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 vectors related to the nsContentUtils::HoldJSObjects function and the nsAutoPtr class, and other vectors.
CVE-2013-0790	Unspecified vulnerability in the browser engine in Mozilla Firefox before 20.0 on Android allows remote attackers to cause a denial of service (stack memory corruption and application crash) or possibly execute arbitrary code via unknown vectors involving a plug-in.
CVE-2013-0792	Mozilla Firefox before 20.0 and SeaMonkey before 2.17, when gfx.color_management.enablev4 is used, do not properly handle color profiles during PNG rendering, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (memory corruption) via a grayscale PNG image.
CVE-2013-0794	Mozilla Firefox before 20.0 and SeaMonkey before 2.17 do not prevent origin spoofing of tab-modal dialogs, which allows remote attackers to conduct phishing attacks via a crafted web site.
CVE-2013-0798	Mozilla Firefox before 20.0 on Android uses world-writable and world-readable permissions for the app_tmp installation directory in the local filesystem, which allows attackers to modify add-ons before installation via an application that leverages the time window during which app_tmp is used.
CVE-2013-1669	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 21.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-1671	Mozilla Firefox before 21.0 does not properly implement the INPUT element, which allows remote attackers to obtain the full pathname via a crafted web site.
CVE-2013-1673	The Mozilla Updater in Mozilla Firefox before 21.0 on Windows does not properly maintain Mozilla Maintenance Service registry entries in certain situations involving upgrades from older Firefox versions, which allows local users to gain privileges by leveraging write access to a "trusted path."
CVE-2013-1683	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 22.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-1688	The Profiler implementation in Mozilla Firefox before 22.0 parses untrusted data during UI rendering, which allows user-assisted remote attackers to execute arbitrary JavaScript code via a crafted web site.
CVE-2013-1695	Mozilla Firefox before 22.0 does not properly implement certain DocShell inheritance behavior for the sandbox attribute of an IFRAME element, which allows remote attackers to bypass intended access restrictions via a FRAME element within an IFRAME element.
CVE-2013-1696	Mozilla Firefox before 22.0 does not properly enforce the X-Frame-Options protection mechanism, which allows remote attackers to conduct clickjacking attacks via a crafted web site that uses the HTTP server push feature with multipart responses.
CVE-2013-1698	The getUserMedia permission implementation in Mozilla Firefox before 22.0 references the URL of a top-level document instead of the URL of a specific page, which makes it easier for remote attackers to trick users into permitting camera or microphone access via a crafted web site that uses IFRAME elements.
CVE-2013-1699	The Internationalized Domain Name (IDN) display algorithm in Mozilla Firefox before 22.0 does not properly handle the .com, .name, and .net top-level domains, which allows remote attackers to spoof the address bar via unspecified homograph characters.
CVE-2013-1700	The Mozilla Maintenance Service in Mozilla Firefox before 22.0 on Windows does not properly handle inability to launch the Mozilla Updater executable file, which allows local users to gain privileges via vectors involving placement of a Trojan horse executable file at an arbitrary location.
CVE-2013-1702	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 23.0 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-2013-1704	Use-after-free vulnerability in the nsINode::GetParentNode function in Mozilla Firefox before 23.0 and SeaMonkey before 2.20 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption and application crash) via vectors involving a DOM modification at the time of a SetBody mutation event.
CVE-2013-1705	Heap-based buffer underflow in the cryptojs_interpret_key_gen_type function in Mozilla Firefox before 23.0 and SeaMonkey before 2.20 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted Certificate Request Message Format (CRMF) request.
CVE-2013-1708	Mozilla Firefox before 23.0 and SeaMonkey before 2.20 allow remote attackers to cause a denial of service (application crash) via a crafted WAV file that is not properly handled by the nsCString::CharAt function.
CVE-2013-1711	The XrayWrapper implementation in Mozilla Firefox before 23.0 and SeaMonkey before 2.20 does not properly address the possibility of an XBL scope bypass resulting from non-native arguments in XBL function calls, which

	makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks by leveraging access to an unprivileged object.
CVE-2013-1715	Multiple untrusted search path vulnerabilities in the (1) full installer and (2) stub installer in Mozilla Firefox before 23.0 on Windows allow local users to gain privileges via a Trojan horse DLL in the default downloads directory. NOTE: this issue exists because of an incomplete fix for CVE-2012-4206.
CVE-2013-1721	Integer overflow in the drawLineLoop function in the libGLESv2 library in Almost Native Graphics Layer Engine (ANGLE), as used in Mozilla Firefox before 24.0 and SeaMonkey before 2.21, allows remote attackers to execute arbitrary code via a crafted web site.
CVE-2013-1727	Mozilla Firefox before 24.0 on Android allows attackers to bypass the Same Origin Policy, and consequently conduct cross-site scripting (XSS) attacks or obtain password or cookie information, by using a symlink in conjunction with a file: URL for a local file.
CVE-2013-1729	The WebGL implementation in Mozilla Firefox before 24.0, when NVIDIA graphics drivers are used on Mac OS X, allows remote attackers to obtain desktop-screenshot data by reading from a CANVAS element.
CVE-2013-1731	Untrusted search path vulnerability in the GL tracing functionality in Mozilla Firefox before 24.0 on Android allows attackers to execute arbitrary code via a Trojan horse .so file in a world-writable directory.
CVE-2013-5592	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 25.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-5598	PDF.js in Mozilla Firefox before 25.0 and Firefox ESR 24.x before 24.1 does not properly handle the appending of an IFRAME element, which allows remote attackers to read arbitrary files or execute arbitrary JavaScript code with chrome privileges by using this element within an embedded PDF object.
CVE-2013-5607	Integer overflow in the PL_ArenaAllocate function in Mozilla Netscape Portable Runtime (NSPR) before 4.10.2, as used in Firefox before 25.0.1, Firefox ESR 17.x before 17.0.11 and 24.x before 24.1.1, and SeaMonkey before 2.22.1, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted X.509 certificate, a related issue to CVE-2013-1741.
CVE-2013-5610	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 26.0 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-2013-5611	Mozilla Firefox before 26.0 does not properly remove the Application Installation doorhanger, which makes it easier for remote attackers to spoof a Web App installation site by controlling the timing of page navigation.
CVE-2013-5612	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 26.0 and SeaMonkey before 2.23 makes it easier for remote attackers to inject arbitrary web script or HTML by leveraging a Same Origin Policy violation triggered by lack of a charset parameter in a Content-Type HTTP header.
CVE-2013-5614	Mozilla Firefox before 26.0 and SeaMonkey before 2.23 do not properly consider the sandbox attribute of an IFRAME element during processing of a contained OBJECT element, which allows remote attackers to bypass intended sandbox restrictions via a crafted web site.
CVE-2013-5619	Multiple integer overflows in the binary-search implementation in SpiderMonkey in Mozilla Firefox before 26.0 and SeaMonkey before 2.23 might allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2013-6167	Mozilla Firefox through 27 sends HTTP Cookie headers without first validating that they have the required character-set restrictions, which allows remote attackers to conduct the equivalent of a persistent Logout CSRF attack via a crafted parameter that forces a web application to set a malformed cookie within an HTTP response.
CVE-2013-6672	Mozilla Firefox before 26.0 and SeaMonkey before 2.23 on Linux allow user-assisted remote attackers to read clipboard data by leveraging certain middle-click paste operations.
CVE-2013-6853	Cross-site scripting (XSS) vulnerability in clickstream.js in Y! Toolbar plugin for FireFox 3.1.0.20130813024103 for Mac, and 2.5.9.2013418100420 for Windows, allows remote attackers to inject arbitrary web script or HTML via a crafted URL that is stored by the victim.
CVE-2013-6901	Cross-site scripting (XSS) vulnerability in the Space function in Cybozu Garoon before 3.7.0, when Firefox is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-6903	Cross-site scripting (XSS) vulnerability in a schedule component in Cybozu Garoon before 3.7.0, when Internet Explorer or Firefox is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-6904	Cross-site scripting (XSS) vulnerability in a note component in Cybozu Garoon before 3.7.0, when Internet Explorer or Firefox is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-6905	Cross-site scripting (XSS) vulnerability in a phone component in Cybozu Garoon before 3.7.0, when Internet Explorer or Firefox is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-6911	Cross-site scripting (XSS) vulnerability in the bulletin-board component in Cybozu Garoon before 3.7.2, when Internet Explorer or Firefox is used, allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.
CVE-2014-0387	Unspecified vulnerability in Oracle Java SE 6u65 and Java SE 7u45, when running on Firefox, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment.

CVE-2014-1478	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0 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 vectors related to the MPostWriteBarrier class in js/src/jit/MIR.h and stack alignment in js/src/jit/AsmJS.cpp in OdinMonkey, and unknown other vectors.
CVE-2014-1480	The file-download implementation in Mozilla Firefox before 27.0 and SeaMonkey before 2.24 does not properly restrict the timing of button selections, which allows remote attackers to conduct clickjacking attacks, and trigger unintended launching of a downloaded file, via a crafted web site.
CVE-2014-1483	Mozilla Firefox before 27.0 and SeaMonkey before 2.24 allow remote attackers to bypass the Same Origin Policy and obtain sensitive information by using an IFRAME element in conjunction with certain timing measurements involving the document.caretPositionFromPoint and document.elementFromPoint functions.
CVE-2014-1484	Mozilla Firefox before 27.0 on Android 4.2 and earlier creates system-log entries containing profile paths, which allows attackers to obtain sensitive information via a crafted application.
CVE-2014-1485	The Content Security Policy (CSP) implementation in Mozilla Firefox before 27.0 and SeaMonkey before 2.24 operates on XSLT stylesheets according to style-src directives instead of script-src directives, which might allow remote attackers to execute arbitrary XSLT code by leveraging insufficient style-src restrictions.
CVE-2014-1488	The Web workers implementation in Mozilla Firefox before 27.0 and SeaMonkey before 2.24 allows remote attackers to execute arbitrary code via vectors involving termination of a worker process that has performed a cross-thread object-passing operation in conjunction with use of asm.js.
CVE-2014-1489	Mozilla Firefox before 27.0 does not properly restrict access to about:home buttons by script on other pages, which allows user-assisted remote attackers to cause a denial of service (session restore) via a crafted web site.
CVE-2014-1494	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0 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-2014-1498	The crypto.generateCRMFRequest method in Mozilla Firefox before 28.0 and SeaMonkey before 2.25 does not properly validate a certain key type, which allows remote attackers to cause a denial of service (application crash) via vectors that trigger generation of a key that supports the Elliptic Curve ec-dual-use algorithm.
CVE-2014-1499	Mozilla Firefox before 28.0 and SeaMonkey before 2.25 allow remote attackers to spoof the domain name in the WebRTC (1) camera or (2) microphone permission prompt by triggering navigation at a certain time during generation of this prompt.
CVE-2014-1500	Mozilla Firefox before 28.0 and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (resource consumption and application hang) via onbeforeunload events that trigger background JavaScript execution.
CVE-2014-1501	Mozilla Firefox before 28.0 on Android allows remote attackers to bypass the Same Origin Policy and access arbitrary file: URLs via vectors involving the "Open Link in New Tab" menu selection.
CVE-2014-1502	The (1) WebGL.compressedTexImage2D and (2) WebGL.compressedTexSubImage2D functions in Mozilla Firefox before 28.0 and SeaMonkey before 2.25 allow remote attackers to bypass the Same Origin Policy and render content in a different domain via unspecified vectors.
CVE-2014-1504	The session-restore feature in Mozilla Firefox before 28.0 and SeaMonkey before 2.25 does not consider the Content Security Policy of a data: URL, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted document that is accessed after a browser restart.
CVE-2014-1506	Directory traversal vulnerability in Android Crash Reporter in Mozilla Firefox before 28.0 on Android allows attackers to trigger the transmission of local files to arbitrary servers, or cause a denial of service (application crash), via a crafted application that specifies Android Crash Reporter arguments.
CVE-2014-1515	Mozilla Firefox before 28.0.1 on Android processes a file: URL by copying a local file onto the SD card, which allows attackers to obtain sensitive information from the Firefox profile directory via a crafted application.
CVE-2014-1516	The saltProfileName function in base/GeckoProfileDirectories.java in Mozilla Firefox through 28.0.1 on Android relies on Android's weak approach to seeding the Math.random function, which makes it easier for attackers to bypass a profile-randomization protection mechanism via a crafted application.
CVE-2014-1519	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0 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-2014-1520	maintenservice_installer.exe in the Maintenance Service Installer in Mozilla Firefox before 29.0 and Firefox ESR 24.x before 24.5 on Windows allows local users to gain privileges by placing a Trojan horse DLL file into a temporary directory at an unspecified point in the update process.
CVE-2014-1522	The mozilla::dom::OscillatorNodeEngine::ComputeCustom function in the Web Audio subsystem in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read, memory corruption, and application crash) via crafted content.
CVE-2014-1525	The mozilla::dom::TextTrack::AddCue function in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 does not properly perform garbage collection for Text Track Manager variables, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and heap memory corruption) via a crafted VIDEO element in an HTML document.

CVE-2014-1526	The XrayWrapper implementation in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allows user-assisted remote attackers to bypass intended access restrictions via a crafted web site that is visited in the debugger, leading to unwrapping operations and calls to DOM methods on the unwrapped objects.
CVE-2014-1527	Mozilla Firefox before 29.0 on Android allows remote attackers to spoof the address bar via crafted JavaScript code that uses DOM events to prevent the reemergence of the actual address bar after scrolling has taken it off of the screen.
CVE-2014-1528	The sse2_composite_src_x888_8888 function in Pixman, as used in Cairo in Mozilla Firefox 28.0 and SeaMonkey 2.25 on Windows, allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write and application crash) by painting on a CANVAS element.
CVE-2014-1533	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 30.0, Firefox ESR 24.x before 24.6, and Thunderbird before 24.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1534	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 30.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1536	The PropertyProvider::FindJustificationRange function in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-1537	Use-after-free vulnerability in the mozilla::dom::WorkerPrivateParent function in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2014-1540	Use-after-free vulnerability in the nsEventListenerManager::CompileEventHandlerInternal function in the Event Listener Manager in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via crafted web content.
CVE-2014-1542	Buffer overflow in the Speex resampler in the Web Audio subsystem in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code via vectors related to a crafted AudioBuffer channel count and sample rate.
CVE-2014-1543	Multiple heap-based buffer overflows in the navigator.getGamepads function in the Gamepad API in Mozilla Firefox before 30.0 allow remote attackers to execute arbitrary code by using non-contiguous axes with a (1) physical or (2) virtual Gamepad device.
CVE-2014-1554	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 32.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1561	Mozilla Firefox before 31.0 does not properly restrict use of drag-and-drop events to spoof customization events, which allows remote attackers to alter the placement of UI icons via crafted JavaScript code that is encountered during (1) page, (2) panel, or (3) toolbar customization.
CVE-2014-1566	Mozilla Firefox before 31.1 on Android does not properly restrict copying of local files onto the SD card during processing of file: URLs, which allows attackers to obtain sensitive information from the Firefox profile directory via a crafted application. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-1515.
CVE-2014-1575	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 33.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to improper interaction between threading and garbage collection in the GCRuntime::triggerGC function in js/src/jsgc.cpp, and unknown other vectors.
CVE-2014-1580	Mozilla Firefox before 33.0 does not properly initialize memory for GIF images, which allows remote attackers to obtain sensitive information from process memory via a crafted web page that triggers a sequence of rendering operations for truncated GIF data within a CANVAS element.
CVE-2014-1582	The Public Key Pinning (PKP) implementation in Mozilla Firefox before 33.0 does not properly consider the connection-coalescing behavior of SPDY and HTTP/2 in the case of a shared IP address, which allows man-in-the-middle attackers to bypass an intended pinning configuration and spoof a web site by providing a valid certificate from an arbitrary recognized Certification Authority.
CVE-2014-1583	The Alarm API in Mozilla Firefox before 33.0 and Firefox ESR 31.x before 31.2 does not properly restrict toJSON calls, which allows remote attackers to bypass the Same Origin Policy via crafted API calls that access sensitive information within the JSON data of an alarm.
CVE-2014-1584	The Public Key Pinning (PKP) implementation in Mozilla Firefox before 33.0 skips pinning checks upon an unspecified issuer-verification error, which makes it easier for remote attackers to bypass an intended pinning configuration and spoof a web site via a crafted certificate that leads to presentation of the Untrusted Connection dialog to the user.
CVE-2014-1588	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 34.0 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-2014-1589	Mozilla Firefox before 34.0 and SeaMonkey before 2.31 provide stylesheets with an incorrect primary namespace, which allows remote attackers to bypass intended access restrictions via an XBL binding.

CVE-2014-1591	Mozilla Firefox 33.0 and SeaMonkey before 2.31 include path strings in CSP violation reports, which allows remote attackers to obtain sensitive information via a web site that receives a report after a redirect.
CVE-2014-6492	Unspecified vulnerability in Oracle Java SE 6u81, 7u67, and 8u20, when running on Firefox, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment.
CVE-2014-8631	The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 34.0 and SeaMonkey before 2.31 supports native-interface passing, which allows remote attackers to bypass intended DOM object restrictions via a call to an unspecified method.
CVE-2014-8632	The structured-clone implementation in Mozilla Firefox before 34.0 and SeaMonkey before 2.31 does not properly interact with XrayWrapper property filtering, which allows remote attackers to bypass intended DOM object restrictions by leveraging property availability after XrayWrapper removal.
CVE-2014-8635	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 35.0 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-2014-8636	The XrayWrapper implementation in Mozilla Firefox before 35.0 and SeaMonkey before 2.32 does not properly interact with a DOM object that has a named getter, which might allow remote attackers to execute arbitrary JavaScript code with chrome privileges via unspecified vectors.
CVE-2014-8637	Mozilla Firefox before 35.0 and SeaMonkey before 2.32 do not properly initialize memory for BMP images, which allows remote attackers to obtain sensitive information from process memory via a crafted web page that triggers the rendering of malformed BMP data within a CANVAS element.
CVE-2014-8640	The mozilla::dom::AudioParamTimeline::AudioNodeInputValue function in the Web Audio API implementation in Mozilla Firefox before 35.0 and SeaMonkey before 2.32 does not properly restrict timeline operations, which allows remote attackers to cause a denial of service (uninitialized-memory read and application crash) via crafted API calls.
CVE-2014-8641	Use-after-free vulnerability in the WebRTC implementation in Mozilla Firefox before 35.0, Firefox ESR 31.x before 31.4, and SeaMonkey before 2.32 allows remote attackers to execute arbitrary code via crafted track data.
CVE-2014-8642	Mozilla Firefox before 35.0 and SeaMonkey before 2.32 do not consider the id-pkix-ocsp-nocheck extension in deciding whether to trust an OCSP responder, which makes it easier for remote attackers to obtain sensitive information by sniffing the network during a session in which there was an incorrect decision to accept a compromised and revoked certificate.
CVE-2014-8643	Mozilla Firefox before 35.0 on Windows allows remote attackers to bypass the Gecko Media Plugin (GMP) sandbox protection mechanism by leveraging access to the GMP process, as demonstrated by the OpenH264 plugin's process.
CVE-2015-0798	The Reader mode feature in Mozilla Firefox before 37.0.1 on Android, and Desktop Firefox pre-release, does not properly handle privileged URLs, which makes it easier for remote attackers to execute arbitrary JavaScript code with chrome privileges by leveraging the ability to bypass the Same Origin Policy.
CVE-2015-0799	The HTTP Alternative Services feature in Mozilla Firefox before 37.0.1 allows man-in-the-middle attackers to bypass an intended X.509 certificate-verification step for an SSL server by specifying that server in the uri-host field of an Alt-Svc HTTP/2 response header.
CVE-2015-0800	The PRNG implementation in the DNS resolver in Mozilla Firefox (aka Fennec) before 37.0 on Android does not properly generate random numbers for query ID values and UDP source ports, which makes it easier for remote attackers to spoof DNS responses by guessing these numbers, a related issue to CVE-2012-2808.
CVE-2015-0802	Mozilla Firefox before 37.0 relies on docshell type information instead of page principal information for Window.webidl access control, which might allow remote attackers to execute arbitrary JavaScript code with chrome privileges via certain content navigation that leverages the reachability of a privileged window with an unintended persistence of access to restricted internal methods.
CVE-2015-0803	The HTMLSourceElement::AfterSetAttr function in Mozilla Firefox before 37.0 does not properly constrain the original data type of a casted value during the setting of a SOURCE element's attributes, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via a crafted HTML document.
CVE-2015-0804	The HTMLSourceElement::BindToTree function in Mozilla Firefox before 37.0 does not properly constrain a data type after omitting namespace validation during certain tree-binding operations, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via a crafted HTML document containing a SOURCE element.
CVE-2015-0805	The Off Main Thread Compositing (OMTC) implementation in Mozilla Firefox before 37.0 makes an incorrect memset call during interaction with the mozilla::layers::BufferTextureClient::AllocateForSurface function, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via vectors that trigger rendering of 2D graphics content.
CVE-2015-0806	The Off Main Thread Compositing (OMTC) implementation in Mozilla Firefox before 37.0 attempts to use memset for a memory region of negative length during interaction with the mozilla::layers::BufferTextureClient::AllocateForSurface function, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors that trigger rendering of 2D graphics content.

CVE-2015-0808	The webrtc::VPMContentAnalysis::Release function in the WebRTC implementation in Mozilla Firefox before 37.0 uses incompatible approaches to the deallocation of memory for simple-type arrays, which might allow remote attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2015-0810	Mozilla Firefox before 37.0 on OS X does not ensure that the cursor is visible, which allows remote attackers to conduct clickjacking attacks via a Flash object in conjunction with DIV elements associated with layered presentation, and crafted JavaScript code that interacts with an IMG element.
CVE-2015-0811	The QCMS implementation in Mozilla Firefox before 37.0 allows remote attackers to obtain sensitive information from process heap memory or cause a denial of service (out-of-bounds read) via an image that is improperly handled during transformation.
CVE-2015-0812	Mozilla Firefox before 37.0 does not require an HTTPS session for lightweight theme add-on installations, which allows man-in-the-middle attackers to bypass an intended user-confirmation requirement by deploying a crafted web site and conducting a DNS spoofing attack against a mozilla.org subdomain.
CVE-2015-0814	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 37.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-0817	The asm.js implementation in Mozilla Firefox before 36.0.3, Firefox ESR 31.x before 31.5.2, and SeaMonkey before 2.33.1 does not properly determine the cases in which bounds checking may be safely skipped during JIT compilation and heap access, which allows remote attackers to read or write to unintended memory locations, and consequently execute arbitrary code, via crafted JavaScript.
CVE-2015-0818	Mozilla Firefox before 36.0.4, Firefox ESR 31.x before 31.5.3, and SeaMonkey before 2.33.1 allow remote attackers to bypass the Same Origin Policy and execute arbitrary JavaScript code with chrome privileges via vectors involving SVG hash navigation.
CVE-2015-0819	The UITour::onPageEvent function in Mozilla Firefox before 36.0 does not ensure that an API call originates from a foreground tab, which allows remote attackers to conduct spoofing and clickjacking attacks by leveraging access to a UI Tour web site.
CVE-2015-0820	Mozilla Firefox before 36.0 does not properly restrict transitions of JavaScript objects from a non-extensible state to an extensible state, which allows remote attackers to bypass a Caja Compiler sandbox protection mechanism or a Secure EcmaScript sandbox protection mechanism via a crafted web site.
CVE-2015-0821	Mozilla Firefox before 36.0 allows user-assisted remote attackers to read arbitrary files or execute arbitrary JavaScript code with chrome privileges via a crafted web site that is accessed with unspecified mouse and keyboard actions.
CVE-2015-0823	Multiple use-after-free vulnerabilities in OpenType Sanitiser, as used in Mozilla Firefox before 36.0, might allow remote attackers to trigger problematic Developer Console information or possibly have unspecified other impact by leveraging incorrect macro expansion, related to the ots::ots_gasp_parse function.
CVE-2015-0824	The mozilla::layers::BufferTextureClient::AllocateForSurface function in Mozilla Firefox before 36.0 allows remote attackers to cause a denial of service (out-of-bounds write of zero values, and application crash) via vectors that trigger use of DrawTarget and the Cairo library for image drawing.
CVE-2015-0825	Stack-based buffer underflow in the mozilla::MP3FrameParser::ParseBuffer function in Mozilla Firefox before 36.0 allows remote attackers to obtain sensitive information from process memory via a malformed MP3 file that improperly interacts with memory allocation during playback.
CVE-2015-0826	The nsTransformedTextRun::SetCapitalization function in Mozilla Firefox before 36.0 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read of heap memory) via a crafted Cascading Style Sheets (CSS) token sequence that triggers a restyle or reflow operation.
CVE-2015-0828	Double free vulnerability in the nsXMLHttpRequest::GetResponse function in Mozilla Firefox before 36.0, when a nonstandard memory allocator is used, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via crafted JavaScript code that makes an XMLHttpRequest call with zero bytes of data.
CVE-2015-0829	Buffer overflow in libstagefright in Mozilla Firefox before 36.0 allows remote attackers to execute arbitrary code via a crafted MP4 video that is improperly handled during playback.
CVE-2015-0830	The WebGL implementation in Mozilla Firefox before 36.0 does not properly allocate memory for copying an unspecified string to a shader's compilation log, which allows remote attackers to cause a denial of service (application crash) via crafted WebGL content.
CVE-2015-0832	Mozilla Firefox before 36.0 does not properly recognize the equivalence of domain names with and without a trailing . (dot) character, which allows man-in-the-middle attackers to bypass the HPKP and HSTS protection mechanisms by constructing a URL with this character and leveraging access to an X.509 certificate for a domain with this character.
CVE-2015-0834	The WebRTC subsystem in Mozilla Firefox before 36.0 recognizes turns: and stuns: URIs but accesses the TURN or STUN server without using TLS, which makes it easier for man-in-the-middle attackers to discover credentials by spoofing a server and completing a brute-force attack within a short time window.
CVE-2015-0835	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 36.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

CVE-2015-2706	Race condition in the AsyncPaintWaitEvent::AsyncPaintWaitEvent function in Mozilla Firefox before 37.0.2 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via a crafted plugin that does not properly complete initialization.
CVE-2015-2709	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 38.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-2711	Mozilla Firefox before 38.0 does not recognize areferrer policy delivered by a referrer META element in cases of context-menu navigation and middle-click navigation, which allows remote attackers to obtain sensitive information by reading web-server Referer logs that contain private data in a URL, as demonstrated by a private path component.
CVE-2015-2712	The asm.js implementation in Mozilla Firefox before 38.0 does not properly determine heap lengths during identification of cases in which bounds checking may be safely skipped, which allows remote attackers to trigger out-of-bounds write operations and possibly execute arbitrary code, or trigger out-of-bounds read operations and possibly obtain sensitive information from process memory, via crafted JavaScript.
CVE-2015-2714	Mozilla Firefox before 38.0 on Android does not properly restrict writing URL data to the Android logging system, which allows attackers to obtain sensitive information via a crafted application that has a required permission for reading a log, as demonstrated by the READ_LOGS permission for the mixed-content violation log on Android 4.0 and earlier.
CVE-2015-2715	Race condition in the nsThreadManager::RegisterCurrentThread function in Mozilla Firefox before 38.0 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and heap memory corruption) by leveraging improper Media Decoder Thread creation at the time of a shutdown.
CVE-2015-2717	Integer overflow in libstagefright in Mozilla Firefox before 38.0 allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and out-of-bounds read) via an MP4 video file containing invalid metadata.
CVE-2015-2718	The WebChannel.jsm module in Mozilla Firefox before 38.0 allows remote attackers to bypass the Same Origin Policy and obtain sensitive webchannel-response data via a crafted web site containing an IFRAME element referencing a different web site that is intended to read this data.
CVE-2015-2720	The update implementation in Mozilla Firefox before 38.0 on Windows does not ensure that the pathname for updater.exe corresponds to the application directory, which might allow local users to gain privileges via a Trojan horse file.
CVE-2015-2722	Use-after-free vulnerability in the CanonicalizeXPComParticipant function in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 allows remote attackers to execute arbitrary code via vectors involving attachment of an XMLHttpRequest object to a shared worker.
CVE-2015-2726	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-2727	Mozilla Firefox 38.0 and Firefox ESR 38.0 allow user-assisted remote attackers to read arbitrary files or execute arbitrary JavaScript code with chrome privileges via a crafted web site that is accessed with unspecified mouse and keyboard actions. NOTE: this vulnerability exists because of a CVE-2015-0821 regression.
CVE-2015-2728	The IndexedDatabaseManager class in the IndexedDB implementation in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 misinterprets an unspecified IDBDatabase field as a pointer, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors, related to a "type confusion" issue.
CVE-2015-2730	Mozilla Network Security Services (NSS) before 3.19.1, as used in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and other products, does not properly perform Elliptical Curve Cryptography (ECC) multiplications, which makes it easier for remote attackers to spoof ECDSA signatures via unspecified vectors.
CVE-2015-2733	Use-after-free vulnerability in the CanonicalizeXPComParticipant function in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 allows remote attackers to execute arbitrary code via vectors involving attachment of an XMLHttpRequest object to a dedicated worker.
CVE-2015-2741	Mozilla Firefox before 39.0, Firefox ESR 38.x before 38.1, and Thunderbird before 38.1 do not enforce key pinning upon encountering an X.509 certificate problem that generates a user dialog, which allows user-assisted man-in-the-middle attackers to bypass intended access restrictions by triggering a (1) expired certificate or (2) mismatched hostname for a domain with pinning enabled.
CVE-2015-2742	Mozilla Firefox before 39.0 on OS X includes native key press information during the logging of crashes, which allows remote attackers to obtain sensitive information by leveraging access to a crash-reporting data stream.
CVE-2015-2743	PDF.js in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 enables excessive privileges for internal Workers, which might allow remote attackers to execute arbitrary code by leveraging a Same Origin Policy bypass.

CVE-2015-4473	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-4474	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 40.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-4475	The mozilla::AudioSink function in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 mishandles inconsistent sample formats within MP3 audio data, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via a malformed file.
CVE-2015-4476	Mozilla Firefox before 41.0 on Android allows user-assisted remote attackers to spoof address-bar attributes by leveraging lack of navigation after a paste of a URL with a nonstandard scheme, as demonstrated by spoofing an SSL attribute.
CVE-2015-4477	Use-after-free vulnerability in the MediaStream playback feature in Mozilla Firefox before 40.0 allows remote attackers to execute arbitrary code via unspecified use of the Web Audio API.
CVE-2015-4478	Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 do not impose certain ECMAScript 6 requirements on JavaScript object properties, which allows remote attackers to bypass the Same Origin Policy via the reviver parameter to the JSON.parse method.
CVE-2015-4479	Multiple integer overflows in libstagefright in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allow remote attackers to execute arbitrary code via a crafted saio chunk in MPEG-4 video data.
CVE-2015-4480	Integer overflow in the stagefright::SampleTable::isValid function in libstagefright in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows remote attackers to execute arbitrary code via crafted MPEG-4 video data with H.264 encoding.
CVE-2015-4481	Race condition in the Mozilla Maintenance Service in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 on Windows allows local users to write to arbitrary files and consequently gain privileges via vectors involving a hard link to a log file during an update.
CVE-2015-4482	mar_read.c in the Updater in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows local users to gain privileges or cause a denial of service (out-of-bounds write) via a crafted name of a Mozilla Archive (aka MAR) file.
CVE-2015-4483	Mozilla Firefox before 40.0 allows man-in-the-middle attackers to bypass a mixed-content protection mechanism via a feed: URL in a POST request.
CVE-2015-4484	The js::jit::AssemblerX86Shared::lock_addl function in the JavaScript implementation in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows remote attackers to cause a denial of service (application crash) by leveraging the use of shared memory and accessing (1) an Atomics object or (2) a SharedArrayBuffer object.
CVE-2015-4485	Heap-based buffer overflow in the resize_context_buffers function in libvpx in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows remote attackers to execute arbitrary code via malformed WebM video data.
CVE-2015-4486	The decrease_ref_count function in libvpx in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via malformed WebM video data.
CVE-2015-4487	The nsTSubstring::ReplacePrep function in Mozilla Firefox before 40.0, Firefox ESR 38.x before 38.2, and Firefox OS before 2.2 might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, related to an "overflow."
CVE-2015-4488	Use-after-free vulnerability in the StyleAnimationValue class in Mozilla Firefox before 40.0, Firefox ESR 38.x before 38.2, and Firefox OS before 2.2 allows remote attackers to have an unspecified impact by leveraging a StyleAnimationValue::operator self assignment.
CVE-2015-4489	The nsTArray_Impl class in Mozilla Firefox before 40.0, Firefox ESR 38.x before 38.2, and Firefox OS before 2.2 might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging a self assignment.
CVE-2015-4490	The nsCSPHostSrc::permits function in dom/security/nsCSPUtils.cpp in Mozilla Firefox before 40.0 does not implement the Content Security Policy Level 2 exceptions for the blob, data, and filesystem URL schemes during wildcard source-expression matching, which might make it easier for remote attackers to conduct cross-site scripting (XSS) attacks by leveraging unexpected policy-enforcement behavior.
CVE-2015-4492	Use-after-free vulnerability in the XMLHttpRequest::Open implementation in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 might allow remote attackers to execute arbitrary code via a SharedWorker object that makes recursive calls to the open method of an XMLHttpRequest object.
CVE-2015-4493	Heap-based buffer overflow in the stagefright::ESDS::parseESDescriptor function in libstagefright in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows remote attackers to execute arbitrary code via an invalid size field in an esds chunk in MPEG-4 video data, a related issue to CVE-2015-1539.
CVE-2015-4495	The PDF reader in Mozilla Firefox before 39.0.3, Firefox ESR 38.x before 38.1.1, and Firefox OS before 2.2 allows remote attackers to bypass the Same Origin Policy, and read arbitrary files or gain privileges, via vectors involving crafted JavaScript code and a native setter, as exploited in the wild in August 2015.

CVE-2015-4496	Multiple integer overflows in libstagefright in Mozilla Firefox before 38.0 allow remote attackers to execute arbitrary code via crafted sample metadata in an MPEG-4 video file, a related issue to CVE-2015-1538.
CVE-2015-4497	Use-after-free vulnerability in the CanvasRenderingContext2D implementation in Mozilla Firefox before 40.0.3 and Firefox ESR 38.x before 38.2.1 allows remote attackers to execute arbitrary code by leveraging improper interaction between resize events and changes to Cascading Style Sheets (CSS) token sequences for a CANVAS element.
CVE-2015-4498	The add-on installation feature in Mozilla Firefox before 40.0.3 and Firefox ESR 38.x before 38.2.1 allows remote attackers to bypass an intended user-confirmation requirement by constructing a crafted data: URL and triggering navigation to an arbitrary http: or https: URL at a certain early point in the installation process.
CVE-2015-4500	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-4501	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 41.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-4502	js/src/proxy/Proxy.cpp in Mozilla Firefox before 41.0 mishandles certain receiver arguments, which allows remote attackers to bypass intended window access restrictions via a crafted web site.
CVE-2015-4503	The TCP Socket API implementation in Mozilla Firefox before 41.0 mishandles array boundaries that were established with a navigator.mozTCPSocket.open method call and send method calls, which allows remote TCP servers to obtain sensitive information from process memory by reading packet data, as demonstrated by availability of this API in a Firefox OS application.
CVE-2015-4504	The lut_inverse_interp16 function in the QCMS library in Mozilla Firefox before 41.0 allows remote attackers to obtain sensitive information or cause a denial of service (buffer over-read and application crash) via crafted attributes in the ICC 4 profile of an image.
CVE-2015-4505	updater.exe in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 on Windows allows local users to write to arbitrary files by conducting a junction attack and waiting for an update operation by the Mozilla Maintenance Service.
CVE-2015-4506	Buffer overflow in the vp9_init_context_buffers function in libvpx, as used in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3, allows remote attackers to execute arbitrary code via a crafted VP9 file.
CVE-2015-4507	The SavedStacks class in the JavaScript implementation in Mozilla Firefox before 41.0, when the Debugger API is enabled, allows remote attackers to cause a denial of service (getSlotRef assertion failure and application exit) or possibly execute arbitrary code via a crafted web site.
CVE-2015-4508	Mozilla Firefox before 41.0, when reader mode is enabled, allows remote attackers to spoof the relationship between address-bar URLs and web content via a crafted web site.
CVE-2015-4509	Use-after-free vulnerability in the HTMLVideoElement interface in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 allows remote attackers to execute arbitrary code via crafted JavaScript code that modifies the URI table of a media element, aka ZDI-CAN-3176.
CVE-2015-4510	Race condition in the WorkerPrivate::NotifyFeatures function in Mozilla Firefox before 41.0 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) by leveraging improper interaction between shared workers and the IndexedDB implementation.
CVE-2015-4511	Heap-based buffer overflow in the nestegg_track_codec_data function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 allows remote attackers to execute arbitrary code via a crafted header in a WebM video.
CVE-2015-4512	gfx/2d/DataSurfaceHelpers.cpp in Mozilla Firefox before 41.0 on Linux improperly attempts to use the Cairo library with 32-bit color-depth surface creation followed by 16-bit color-depth surface display, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) by using a CANVAS element to trigger 2D rendering.
CVE-2015-4513	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-4514	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 42.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-4515	Mozilla Firefox before 42.0, when NTLM v1 is enabled for HTTP authentication, allows remote attackers to obtain sensitive hostname information by constructing a crafted web site that sends an NTLM request and reads the Workstation field of an NTLM type 3 message.
CVE-2015-4516	Mozilla Firefox before 41.0 allows remote attackers to bypass certain ECMAScript 5 (aka ES5) API protection mechanisms and modify immutable properties, and consequently execute arbitrary JavaScript code with chrome privileges, via a crafted web page that does not use ES5 APIs.
CVE-2015-4517	NetworkUtils.cpp in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.

CVE-2015-4518	The Reader View implementation in Mozilla Firefox before 42.0 has an improper whitelist, which makes it easier for remote attackers to bypass the Content Security Policy (CSP) protection mechanism and conduct cross-site scripting (XSS) attacks via vectors involving SVG animations and the about:reader URL.
CVE-2015-4519	Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 allow user-assisted remote attackers to bypass intended access restrictions and discover a redirect's target URL via crafted JavaScript code that executes after a drag-and-drop action of an image into a TEXTBOX element.
CVE-2015-4520	Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 allow remote attackers to bypass CORS preflight protection mechanisms by leveraging (1) duplicate cache-key generation or (2) retrieval of a value from an incorrect HTTP Access-Control-* response header.
CVE-2015-4521	The ConvertDialogOptions function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2015-4522	The nsUnicodeToUTF8::GetMaxLength function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors, related to an "overflow."
CVE-2015-7174	The nsAttrAndChildArray::GrowBy function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors, related to an "overflow."
CVE-2015-7175	The XULContentSinkImpl::AddText function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors, related to an "overflow."
CVE-2015-7176	The AnimationThread function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 uses an incorrect argument to the sscanf function, which might allow remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2015-7177	The InitTextures function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2015-7178	The ProgramBinary::linkAttributes function in libGLES in ANGLE, as used in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 on Windows, mishandles shader access, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted (1) OpenGL or (2) WebGL content.
CVE-2015-7179	The VertexBufferInterface::reserveVertexSpace function in libGLES in ANGLE, as used in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 on Windows, incorrectly allocates memory for shader attribute arrays, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via crafted (1) OpenGL or (2) WebGL content.
CVE-2015-7180	The ReadbackResultWriterD3D11::Run function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 misinterprets the return value of a function call, which might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2015-7181	The sec_asn1d_parse_leaf function in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, improperly restricts access to an unspecified data structure, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data, related to a "use-after-poison" issue.
CVE-2015-7182	Heap-based buffer overflow in the ASN.1 decoder in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data.
CVE-2015-7183	Integer overflow in the PL_ARENA_ALLOCATE implementation in Netscape Portable Runtime (NSPR) in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.
CVE-2015-7184	The fetch API implementation in Mozilla Firefox before 41.0.2 does not restrict access to the HTTP response body in certain situations where user credentials are supplied but the CORS cross-origin request algorithm is improperly followed, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2015-7185	Mozilla Firefox before 42.0 on Android does not ensure that the address bar is restored upon fullscreen-mode exit, which allows remote attackers to spoof the address bar via crafted JavaScript code.
CVE-2015-7186	Mozilla Firefox before 42.0 on Android allows user-assisted remote attackers to bypass the Same Origin Policy and trigger (1) a download or (2) cached profile-data reading via a file: URL in a saved HTML document.
CVE-2015-7187	The Add-on SDK in Mozilla Firefox before 42.0 misinterprets a "script: false" panel setting, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via inline JavaScript code that is executed within a third-party extension.

CVE-2015-7188	Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allow remote attackers to bypass the Same Origin Policy for an IP address origin, and conduct cross-site scripting (XSS) attacks, by appending whitespace characters to an IP address string.
CVE-2015-7189	Race condition in the JPEGEncoder function in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow) via vectors involving a CANVAS element and crafted JavaScript code.
CVE-2015-7190	The Search feature in Mozilla Firefox before 42.0 on Android through 4.4 supports search-engine URL registration through an intent and can access this URL in a privileged context in conjunction with the crash reporter, which allows attackers to read log files and visit file: URLs of HTML documents via a crafted application.
CVE-2015-7191	Mozilla Firefox before 42.0 on Android improperly restricts URL strings in intents, which allows attackers to conduct cross-site scripting (XSS) attacks via vectors involving an intent: URL and fallback navigation, aka "Universal XSS (UXSS)."
CVE-2015-7192	The accessibility-tools feature in Mozilla Firefox before 42.0 on OS X improperly interacts with the implementation of the TABLE element, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by using an NSAccessibilityIndexAttribute value to reference a row index.
CVE-2015-7193	Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 improperly follow the CORS cross-origin request algorithm for the POST method in situations involving an unspecified Content-Type header manipulation, which allows remote attackers to bypass the Same Origin Policy by leveraging the lack of a preflight-request step.
CVE-2015-7194	Buffer underflow in libjar in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted ZIP archive.
CVE-2015-7195	The URL parsing implementation in Mozilla Firefox before 42.0 improperly recognizes escaped characters in hostnames within Location headers, which allows remote attackers to obtain sensitive information via vectors involving a redirect.
CVE-2015-7196	Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4, when a Java plugin is enabled, allow remote attackers to cause a denial of service (incorrect garbage collection and application crash) or possibly execute arbitrary code via a crafted Java applet that deallocates an in-use JavaScript wrapper.
CVE-2015-7197	Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 improperly control the ability of a web worker to create a WebSocket object, which allows remote attackers to bypass intended mixed-content restrictions via crafted JavaScript code.
CVE-2015-7198	Buffer overflow in the rx::TextureStorage11 class in ANGLE, as used in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted texture data.
CVE-2015-7199	The (1) AddWeightedPathSegLists and (2) SVGPathSegListSMILType::Interpolate functions in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 lack status checking, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted SVG document.
CVE-2015-7200	The CryptoKey interface implementation in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 lacks status checking, which allows attackers to have an unspecified impact via vectors related to a cryptographic key.
CVE-2015-7201	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-7202	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 43.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-7203	Buffer overflow in the DirectWriteFontInfo::LoadFontFamilyData function in gfx/thebes/gfxDWriteFontList.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted font-family name.
CVE-2015-7204	Mozilla Firefox before 43.0 does not properly store the properties of unboxed objects, which allows remote attackers to execute arbitrary code via crafted JavaScript variable assignments.
CVE-2015-7205	Integer underflow in the RTPReceiverVideo::ParseRtpPacket function in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 might allow remote attackers to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a crafted WebRTC RTP packet.
CVE-2015-7207	Mozilla Firefox before 43.0 does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via crafted JavaScript code that leverages history.back and performance.getEntries calls, a related issue to CVE-2015-1300.
CVE-2015-7208	Mozilla Firefox before 43.0 stores cookies containing vertical tab characters, which allows remote attackers to obtain sensitive information by reading HTTP Cookie headers.
CVE-2015-7210	Use-after-free vulnerability in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allows remote attackers to execute arbitrary code by triggering attempted use of a data channel that has been closed by a WebRTC function.
CVE-2015-7211	Mozilla Firefox before 43.0 mishandles the # (number sign) character in a data: URI, which allows remote attackers to spoof web sites via unspecified vectors.

CVE-2015-7212	Integer overflow in the mozilla::layers::BufferTextureClient::AllocateForSurface function in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allows remote attackers to execute arbitrary code by triggering a graphics operation that requires a large texture allocation.
CVE-2015-7213	Integer overflow in the MPEG4Extractor::readMetaData function in MPEG4Extractor.cpp in libstagefright in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 on 64-bit platforms allows remote attackers to execute arbitrary code via a crafted MP4 video file that triggers a buffer overflow.
CVE-2015-7214	Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allow remote attackers to bypass the Same Origin Policy via data: and view-source: URIs.
CVE-2015-7215	The importScripts function in the Web Workers API implementation in Mozilla Firefox before 43.0 allows remote attackers to bypass the Same Origin Policy by triggering use of the no-cors mode in the fetch API to attempt resource access that throws an exception, leading to information disclosure after a rethrow.
CVE-2015-7216	The gdk-pixbuf configuration in Mozilla Firefox before 43.0 on Linux GNOME platforms incorrectly enables the JasPer decoder, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JPEG 2000 image.
CVE-2015-7217	The gdk-pixbuf configuration in Mozilla Firefox before 43.0 on Linux GNOME platforms incorrectly enables the TGA decoder, which allows remote attackers to cause a denial of service (heap-based buffer overflow) via a crafted Truevision TGA image.
CVE-2015-7218	The HTTP/2 implementation in Mozilla Firefox before 43.0 allows remote attackers to cause a denial of service (integer underflow, assertion failure, and application exit) via a single-byte header frame that triggers incorrect memory allocation.
CVE-2015-7219	The HTTP/2 implementation in Mozilla Firefox before 43.0 allows remote attackers to cause a denial of service (integer underflow, assertion failure, and application exit) via a malformed PushPromise frame that triggers decompressed-buffer length miscalculation and incorrect memory allocation.
CVE-2015-7220	Buffer overflow in the XDRBuffer::grow function in js/src/vm/Xdr.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.
CVE-2015-7221	Buffer overflow in the nsDeque::GrowCapacity function in xpcom/glue/nsDeque.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a deque size change.
CVE-2015-7222	Integer underflow in the Metadata::setData function in MetaData.cpp in libstagefright in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allows remote attackers to execute arbitrary code or cause a denial of service (incorrect memory allocation and application crash) via an MP4 video file with crafted covr metadata that triggers a buffer overflow.
CVE-2015-7223	The WebExtension APIs in Mozilla Firefox before 43.0 allow remote attackers to gain privileges, and possibly obtain sensitive information or conduct cross-site scripting (XSS) attacks, via a crafted web site.
CVE-2015-7327	Mozilla Firefox before 41.0 does not properly restrict the availability of High Resolution Time API times, which allows remote attackers to track last-level cache access, and consequently obtain sensitive information, via crafted JavaScript code that makes performance.now calls.
CVE-2015-7575	Mozilla Network Security Services (NSS) before 3.20.2, as used in Mozilla Firefox before 43.0.2 and Firefox ESR 38.x before 38.5.2, does not reject MD5 signatures in Server Key Exchange messages in TLS 1.2 Handshake Protocol traffic, which makes it easier for man-in-the-middle attackers to spoof servers by triggering a collision.
CVE-2016-1930	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 44.0 and Firefox ESR 38.x before 38.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-1931	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 44.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to uninitialized memory encountered during brotli data compression, and other vectors.
CVE-2016-1933	Integer overflow in the image-deinterlacing functionality in Mozilla Firefox before 44.0 allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted GIF image.
CVE-2016-1935	Buffer overflow in the BufferSubData function in Mozilla Firefox before 44.0 and Firefox ESR 38.x before 38.6 allows remote attackers to execute arbitrary code via crafted WebGL content.
CVE-2016-1937	The protocol-handler dialog in Mozilla Firefox before 44.0 allows remote attackers to conduct clickjacking attacks via a crafted web site that triggers a single-click action in a situation where a double-click action was intended.
CVE-2016-1938	The s_mp_div function in lib/freebl/mpi/mpic.c in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, improperly divides numbers, which might make it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging use of the (1) mp_div or (2) mp_exptmod function.
CVE-2016-1939	Mozilla Firefox before 44.0 stores cookies with names containing vertical tab characters, which allows remote attackers to obtain sensitive information by reading HTTP Cookie headers. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-7208.
CVE-2016-1940	Mozilla Firefox before 44.0 on Android allows remote attackers to spoof the address bar via a data: URL that is mishandled during (1) shortcut opening or (2) BOOKMARK intent processing.

CVE-2016-1941	The file-download dialog in Mozilla Firefox before 44.0 on OS X enables a certain button too quickly, which allows remote attackers to conduct clickjacking attacks via a crafted web site that triggers a single-click action in a situation where a double-click action was intended.
CVE-2016-1942	Mozilla Firefox before 44.0 allows user-assisted remote attackers to spoof a trailing substring in the address bar by leveraging a user's paste of a (1) wyciwyg: URI or (2) resource: URI.
CVE-2016-1943	Mozilla Firefox before 44.0 on Android allows remote attackers to spoof the address bar via the scrollTo method.
CVE-2016-1944	The Buffer11::NativeBuffer11::map function in ANGLE, as used in Mozilla Firefox before 44.0, might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1945	The nsZipArchive function in Mozilla Firefox before 44.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect use of a pointer during processing of a ZIP archive.
CVE-2016-1946	The MoofParser::Metadata function in binding/MoofParser.cpp in libstagefright in Mozilla Firefox before 44.0 does not limit the size of read operations, which might allow remote attackers to cause a denial of service (integer overflow and buffer overflow) or possibly have unspecified other impact via crafted metadata.
CVE-2016-1947	Mozilla Firefox 43.x mishandles attempts to connect to the Application Reputation service, which makes it easier for remote attackers to trigger an unintended download by leveraging the absence of reputation data.
CVE-2016-1948	Mozilla Firefox before 44.0 on Android does not ensure that HTTPS is used for a lightweight-theme installation, which allows man-in-the-middle attackers to replace a theme's images and colors by modifying the client-server data stream.
CVE-2016-1949	Mozilla Firefox before 44.0.2 does not properly restrict the interaction between Service Workers and plugins, which allows remote attackers to bypass the Same Origin Policy via a crafted web site that triggers spoofed responses to requests that use NPAPI, as demonstrated by a request for a crossdomain.xml file.
CVE-2016-1950	Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x before 3.21.1, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to execute arbitrary code via crafted ASN.1 data in an X.509 certificate.
CVE-2016-1955	Mozilla Firefox before 45.0 allows remote attackers to bypass the Same Origin Policy and obtain sensitive information by reading a Content Security Policy (CSP) violation report that contains path information associated with an IFRAME element.
CVE-2016-1956	Mozilla Firefox before 45.0 on Linux, when an Intel video driver is used, allows remote attackers to cause a denial of service (memory consumption or stack memory corruption) by triggering use of a WebGL shader.
CVE-2016-1958	browser/base/content/browser.js in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to spoof the address bar via a javascript: URL.
CVE-2016-1959	The ServiceWorkerManager class in Mozilla Firefox before 45.0 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via unspecified use of the Clients API.
CVE-2016-1962	Use-after-free vulnerability in the mozilla::DataChannelConnection::Close function 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 WebRTC data-channel connections.
CVE-2016-1963	The FileReader class in Mozilla Firefox before 45.0 allows local users to gain privileges or cause a denial of service (memory corruption) by changing a file during a FileReader API read operation.
CVE-2016-1965	Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 mishandle a navigation sequence that returns to the original page, which allows remote attackers to spoof the address bar via vectors involving the history.back method and the location.protocol property.
CVE-2016-1967	Mozilla Firefox before 45.0 does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via crafted JavaScript code that leverages history.back and performance.getEntries calls after restoring a browser session. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-7207.
CVE-2016-1968	Integer underflow in Brotli, as used in Mozilla Firefox before 45.0, allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via crafted data with brotli compression.
CVE-2016-1969	The setAttr function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.6.1, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-1970	Integer underflow in the srtp_unprotect function in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1971	The I420VideoFrame::CreateFrame function in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows omits an unspecified status check, which might allow remote attackers to cause a denial of service (memory corruption) or possibly have other impact via unknown vectors.
CVE-2016-1972	Race condition in libvpx in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.

CVE-2016-1973	Race condition in the GetStaticInstance function in the WebRTC implementation in Mozilla Firefox before 45.0 might allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via unspecified vectors.
CVE-2016-1975	Multiple race conditions in dom/media/systemservices/CamerasChild.cpp in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1976	Use-after-free vulnerability in the DesktopDisplayDevice class in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1977	The Machine::Code::decoder::analysis::set_ref function in Graphite 2 before 1.3.6, as used 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 (stack memory corruption) via a crafted Graphite smart font.
CVE-2016-1978	Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact by making an SSL (1) DHE or (2) ECDHE handshake at a time of high memory consumption.
CVE-2016-1979	Use-after-free vulnerability in the PK11_ImportDERPrivateKeyInfoAndReturnKey function in Mozilla Network Security Services (NSS) before 3.21.1, as used in Mozilla Firefox before 45.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted key data with DER encoding.
CVE-2016-2790	The graphite2::TtfUtil::GetTableInfo function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, does not initialize memory for an unspecified data structure, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted Graphite smart font.
CVE-2016-2791	The graphite2::GlyphCache::glyph function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2792	The graphite2::Slot::getAttr function in Slot.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2800.
CVE-2016-2793	CachedCmap.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2794	The graphite2::TtfUtil::CmapSubtable12NextCodepoint function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2795	The graphite2::FileFace::get_table_fn function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, does not initialize memory for an unspecified data structure, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted Graphite smart font.
CVE-2016-2796	Heap-based buffer overflow in the graphite2::vm::Machine::Code function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2797	The graphite2::TtfUtil::CmapSubtable12Lookup function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2801.
CVE-2016-2798	The graphite2::GlyphCache::Loader::Loader function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2799	Heap-based buffer overflow in the graphite2::Slot::setAttr function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2800	The graphite2::Slot::getAttr function in Slot.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2792.
CVE-2016-2801	The graphite2::TtfUtil::CmapSubtable12Lookup function in TtfUtil.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2797.

CVE-2016-2802	The graphite2::TtfUtil::CmapSubtable4NextCodepoint function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
---------------	---

## OfBiz CVEs

cve_id	description
CVE-2012-1622	Apache OFBiz 10.04.x before 10.04.02 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0232	Multiple cross-site scripting (XSS) vulnerabilities in framework/common/webcommon/includes/messages.ftl in Apache OFBiz 11.04.01 before 11.04.05 and 12.04.01 before 12.04.04 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, which are not properly handled in a (1) result or (2) error message.
CVE-2015-3268	Cross-site scripting (XSS) vulnerability in the DisplayEntityField.getDescription method in ModelFormField.java in Apache OFBiz before 12.04.06 and 13.07.x before 13.07.03 allows remote attackers to inject arbitrary web script or HTML via the description attribute of a display-entity element.
CVE-2016-2170	Apache OFBiz 12.04.x before 12.04.06 and 13.07.x before 13.07.03 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library.
CVE-2016-4462	By manipulating the URL parameter externalLoginKey, a malicious, logged in user could pass valid Freemarker directives to the Template Engine that are reflected on the webpage; a specially crafted Freemarker template could be used for remote code execution. Mitigation: Upgrade to Apache OFBiz 16.11.01
CVE-2016-6800	The default configuration of the OFBiz framework offers a blog functionality. Different users are able to operate blogs which are related to specific parties. In the form field for the creation of new blog articles the user input of the summary field as well as the article field is not properly sanitized. It is possible to inject arbitrary JavaScript code in these form fields. This code gets executed from the browser of every user who is visiting this article. Mitigation: Upgrade to Apache OFBiz 16.11.01.
CVE-2017-15714	The BIRT plugin in Apache OFBiz 16.11.01 to 16.11.03 does not escape user input property passed. This allows for code injection by passing that code through the URL. For example by appending this code "__format=%27;alert(%27xss%27)" to the URL an alert window would execute.

## OpenMRS CVEs

cve_id	description
CVE-2014-8071	Multiple cross-site scripting (XSS) vulnerabilities in OpenMRS 2.1 Standalone Edition allow remote attackers to inject arbitrary web script or HTML via the (1) givenName, (2) familyName, (3) address1, or (4) address2 parameter to registrationapp/registerPatient.page; the (5) comment parameter to allergyui/allergy.page; the (6) w10 parameter to htmlformentryui/htmlform/enterHtmlForm/submit.action; the (7) HTTP Referer Header to login.htm; the (8) returnUrl parameter to htmlformentryui/htmlform/enterHtmlFormWithStandardUi.page or (9) coreapps/mergeVisits.page; or the (10) visitId parameter to htmlformentryui/htmlform/enterHtmlFormWithSimpleUi.page.
CVE-2014-8072	The administration module in OpenMRS 2.1 Standalone Edition allows remote authenticated users to obtain read access via a direct request to /admin.
CVE-2014-8073	Cross-site request forgery (CSRF) vulnerability in OpenMRS 2.1 Standalone Edition allows remote attackers to hijack the authentication of administrators for requests that add a new user via a Save User action to admin/users/user.form.

CVE-2017-12796	The Reporting Compatibility Add On before 2.0.4 for OpenMRS, as distributed in OpenMRS Reference Application before 2.6.1, does not authenticate users when deserializing XML input into ReportSchema objects. The result is that remote unauthenticated users are able to execute operating system commands by crafting malicious XML payloads, as demonstrated by a single admin/reports/reportSchemaXml.form request.
----------------	--

## Pidgin CVEs

cve_id	description
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-2014-3698	The jabber_idn_validate function in jutil.c in the Jabber protocol plugin in libpurple in Pidgin before 2.10.10 allows remote attackers to obtain sensitive information from process memory via a crafted XMPP message.
CVE-2014-3697	Absolute path traversal vulnerability in the untar_block function in win32/untar.c in Pidgin before 2.10.10 on Windows allows remote attackers to write to arbitrary files via a drive name in a tar archive of a smiley theme.
CVE-2014-3696	nmevent.c in the Novell GroupWise protocol plugin in libpurple in Pidgin before 2.10.10 allows remote servers to cause a denial of service (application crash) via a crafted server message that triggers a large memory allocation.
CVE-2014-3695	markup.c in the MXit protocol plugin in libpurple in Pidgin before 2.10.10 allows remote servers to cause a denial of service (application crash) via a large length value in an emoticon response.
CVE-2014-3694	The (1) bundled GnuTLS SSL/TLS plugin and the (2) bundled OpenSSL SSL/TLS plugin in libpurple in Pidgin before 2.10.10 do not properly consider the Basic Constraints extension during verification of X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2013-6490	The SIMPLE protocol functionality in Pidgin before 2.10.8 allows remote attackers to have an unspecified impact via a negative Content-Length header, which triggers a buffer overflow.
CVE-2013-6489	Integer signedness error in the MXit functionality in Pidgin before 2.10.8 allows remote attackers to cause a denial of service (segmentation fault) via a crafted emoticon value, which triggers an integer overflow and a buffer overflow.
CVE-2013-6487	Integer overflow in libpurple/protocols/gg/lib/http.c in the Gadu-Gadu (gg) parser in Pidgin before 2.10.8 allows remote attackers to have an unspecified impact via a large Content-Length value, which triggers a buffer overflow.
CVE-2013-6482	Pidgin before 2.10.8 allows remote MSN servers to cause a denial of service (NULL pointer dereference and crash) via a crafted (1) SOAP response, (2) OIM XML response, or (3) Content-Length header.
CVE-2013-6481	libpurple/protocols/yahoo/libymsg.c in Pidgin before 2.10.8 allows remote attackers to cause a denial of service (crash) via a Yahoo! P2P message with a crafted length field, which triggers a buffer over-read.
CVE-2014-0020	The IRC protocol plugin in libpurple in Pidgin before 2.10.8 does not validate argument counts, which allows remote IRC servers to cause a denial of service (application crash) via a crafted message.
CVE-2013-6486	gtkutils.c in Pidgin before 2.10.8 on Windows allows user-assisted remote attackers to execute arbitrary programs via a message containing a file: URL that is improperly handled during construction of an explorer.exe command. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3185.
CVE-2013-6485	Buffer overflow in util.c in libpurple in Pidgin before 2.10.8 allows remote HTTP servers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid chunk-size field in chunked transfer-coding data.
CVE-2013-6484	The STUN protocol implementation in libpurple in Pidgin before 2.10.8 allows remote STUN servers to cause a denial of service (out-of-bounds write operation and application crash) by triggering a socket read error.
CVE-2013-6483	The XMPP protocol plugin in libpurple in Pidgin before 2.10.8 does not properly determine whether the from address in an iq reply is consistent with the to address in an iq request, which allows remote attackers to spoof iq traffic or cause a denial of service (NULL pointer dereference and application crash) via a crafted reply.
CVE-2013-6479	util.c in libpurple in Pidgin before 2.10.8 does not properly allocate memory for HTTP responses that are inconsistent with the Content-Length header, which allows remote HTTP servers to cause a denial of service (application crash) via a crafted response.
CVE-2013-6478	gtkimhtml.c in Pidgin before 2.10.8 does not properly interact with underlying library support for wide Pango layouts, which allows user-assisted remote attackers to cause a denial of service (application crash) via a long URL that is examined with a tooltip.
CVE-2013-6477	Multiple integer signedness errors in libpurple in Pidgin before 2.10.8 allow remote attackers to cause a denial of service (application crash) via a crafted timestamp value in an XMPP message.
CVE-2012-6152	The Yahoo! protocol plugin in libpurple in Pidgin before 2.10.8 does not properly validate UTF-8 data, which allows remote attackers to cause a denial of service (application crash) via crafted byte sequences.

CVE-2013-0274	upnp.c in libpurple in Pidgin before 2.10.7 does not properly terminate long strings in UPnP responses, which allows remote attackers to cause a denial of service (application crash) by leveraging access to the local network.
CVE-2013-0273	sametime.c in the Sametime protocol plugin in libpurple in Pidgin before 2.10.7 does not properly terminate long user IDs, which allows remote servers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-0272	Buffer overflow in http.c in the MXit protocol plugin in libpurple in Pidgin before 2.10.7 allows remote servers to execute arbitrary code via a long HTTP header.
CVE-2013-0271	The MXit protocol plugin in libpurple in Pidgin before 2.10.7 might allow remote attackers to create or overwrite files via a crafted (1) mxit or (2) mxit/imagestrips pathname.
CVE-2011-4922	cipher.c in the Cipher API in libpurple in Pidgin before 2.7.10 retains encryption-key data in process memory, which might allow local users to obtain sensitive information by reading a core file or other representation of memory contents.
CVE-2012-3374	Buffer overflow in markup.c in the MXit protocol plugin in libpurple in Pidgin before 2.10.5 allows remote attackers to execute arbitrary code via a crafted inline image in a message.
CVE-2012-2318	msg.c in the MSN protocol plugin in libpurple in Pidgin before 2.10.4 does not properly handle crafted characters, which allows remote servers to cause a denial of service (application crash) by placing these characters in a text/plain message.
CVE-2012-2214	proxy.c in libpurple in Pidgin before 2.10.4 does not properly handle canceled SOCKS5 connection attempts, which allows user-assisted remote authenticated users to cause a denial of service (application crash) via a sequence of XMPP file-transfer requests.
CVE-2012-2369	Format string vulnerability in the log_message_cb function in otr-plugin.c in the Off-the-Record Messaging (OTR) pidgin-otr plugin before 3.2.1 for Pidgin might allow remote attackers to execute arbitrary code via format string specifiers in data that generates a log message.
CVE-2012-1178	The msn_oim_report_to_user function in oim.c in the MSN protocol plugin in libpurple in Pidgin before 2.10.2 allows remote servers to cause a denial of service (application crash) via an OIM message that lacks UTF-8 encoding.
CVE-2011-4939	The pidgin_conv_chat_rename_user function in gtkconv.c in Pidgin before 2.10.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) by changing a nickname while in an XMPP chat room.
CVE-2011-4601	family_feedbag.c in the oscar protocol plugin in libpurple in Pidgin before 2.10.1 does not perform the expected UTF-8 validation on message data, which allows remote attackers to cause a denial of service (application crash) via a crafted (1) AIM or (2) ICQ message associated with buddy-list addition.
CVE-2011-4603	The silc_channel_message function in ops.c in the SILC protocol plugin in libpurple in Pidgin before 2.10.1 does not perform the expected UTF-8 validation on message data, which allows remote attackers to cause a denial of service (application crash) via a crafted message, a different vulnerability than CVE-2011-3594.
CVE-2011-4602	The XMPP protocol plugin in libpurple in Pidgin before 2.10.1 does not properly handle missing fields in (1) voice-chat and (2) video-chat stanzas, which allows remote attackers to cause a denial of service (application crash) via a crafted message.
CVE-2011-3594	The g_markup_escape_text function in the SILC protocol plug-in in libpurple 2.10.0 and earlier, as used in Pidgin and possibly other products, allows remote attackers to cause a denial of service (crash) via invalid UTF-8 sequences that trigger use of invalid pointers and an out-of-bounds read, related to interactions with certain versions of glib2.
CVE-2011-3185	gtkutils.c in Pidgin before 2.10.0 on Windows allows user-assisted remote attackers to execute arbitrary programs via a file: URL in a message.
CVE-2011-3184	The msn_httpconn_parse_data function in httpconn.c in the MSN protocol plugin in libpurple in Pidgin before 2.10.0 does not properly handle HTTP 100 responses, which allows remote attackers to cause a denial of service (incorrect memory access and application crash) via vectors involving a crafted server message.
CVE-2011-2943	The irc_msg_who function in msgs.c in the IRC protocol plugin in libpurple 2.8.0 through 2.9.0 in Pidgin before 2.10.0 does not properly validate characters in nicknames, which allows user-assisted remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted nickname that is not properly handled in a WHO response.
CVE-2011-1091	libymsg.c in the Yahoo! protocol plugin in libpurple in Pidgin 2.6.0 through 2.7.10 allows (1) remote authenticated users to cause a denial of service (NULL pointer dereference and application crash) via a malformed YMSG notification packet, and allows (2) remote Yahoo! servers to cause a denial of service (NULL pointer dereference and application crash) via a malformed YMSG SMS message.
CVE-2010-4528	directconn.c in the MSN protocol plugin in libpurple 2.7.6 through 2.7.8 in Pidgin before 2.7.9 allows remote authenticated users to cause a denial of service (NULL pointer dereference and application crash) via a short p2pv2 packet in a DirectConnect (aka direct connection) session.
CVE-2010-3711	libpurple in Pidgin before 2.7.4 does not properly validate the return value of the purple_base64_decode function, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and application crash) via a crafted message, related to the plugins for MSN, MySpaceIM, XMPP, and Yahoo! and the NTLM authentication support.

CVE-2010-3088	The notify function in pidgin-knotify.c in the pidgin-knotify plugin 0.2.1 and earlier for Pidgin allows remote attackers to execute arbitrary commands via shell metacharacters in a message.
CVE-2010-2528	The clientautoresp function in family_icbm.c in the oscar protocol plugin in libpurple in Pidgin before 2.7.2 allows remote authenticated users to cause a denial of service (NULL pointer dereference and application crash) via an X-Status message that lacks the expected end tag for a (1) desc or (2) title element.
CVE-2010-1624	The msn_emoticon_msg function in slp.c in the MSN protocol plugin in libpurple in Pidgin before 2.7.0 allows remote authenticated users to cause a denial of service (NULL pointer dereference and application crash) via a custom emoticon in a malformed SLP message.
CVE-2010-0423	gtkimhtml.c in Pidgin before 2.6.6 allows remote attackers to cause a denial of service (CPU consumption and application hang) by sending many smileys in a (1) IM or (2) chat.
CVE-2010-0420	libpurple in Finch in Pidgin before 2.6.6, when an XMPP multi-user chat (MUC) room is used, does not properly parse nicknames containing   sequences, which allows remote attackers to cause a denial of service (application crash) via a crafted nickname.
CVE-2010-0277	slp.c in the MSN protocol plugin in libpurple in Pidgin before 2.6.6, including 2.6.4, and Adium 1.3.8 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed MSNSLP INVITE request in an SLP message, a different issue than CVE-2010-0013.
CVE-2010-0013	Directory traversal vulnerability in slp.c in the MSN protocol plugin in libpurple in Pidgin 2.6.4 and Adium 1.3.8 allows remote attackers to read arbitrary files via a .. (dot dot) in an application/x-msnmssgrp2p MSN emoticon (aka custom smiley) request, a related issue to CVE-2004-0122. NOTE: it could be argued that this is resultant from a vulnerability in which an emoticon download request is processed even without a preceding text/x-mms-emoticon message that announced availability of the emoticon.
CVE-2009-3615	The OSCAR protocol plugin in libpurple in Pidgin before 2.6.3 and Adium before 1.3.7 allows remote attackers to cause a denial of service (application crash) via crafted contact-list data for (1) ICQ and possibly (2) AIM, as demonstrated by the SIM IM client.
CVE-2009-3085	The XMPP protocol plugin in libpurple in Pidgin before 2.6.2 does not properly handle an error IQ stanza during an attempted fetch of a custom smiley, which allows remote attackers to cause a denial of service (application crash) via XHTML-IM content with cid: images.
CVE-2009-3084	The msn_slp_process_msg function in libpurple/protocols/msn/slpcall.c in the MSN protocol plugin in libpurple 2.6.0 and 2.6.1, as used in Pidgin before 2.6.2, allows remote attackers to cause a denial of service (application crash) via a handwritten (aka Ink) message, related to an uninitialized variable and the incorrect "UTF16-LE" charset name.
CVE-2009-3083	The msn_slp_sip_recv function in libpurple/protocols/msn/slpcall.c in the MSN protocol plugin in libpurple in Pidgin before 2.6.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an SLP invite message that lacks certain required fields, as demonstrated by a malformed message from a KMess client.
CVE-2009-2703	libpurple/protocols/irc/msg.c in the IRC protocol plugin in libpurple in Pidgin before 2.6.2 allows remote IRC servers to cause a denial of service (NULL pointer dereference and application crash) via a TOPIC message that lacks a topic string.
CVE-2009-3026	protocols/jabber/auth.c in libpurple in Pidgin 2.6.0, and possibly other versions, does not follow the "require TLS/SSL" preference when connecting to older Jabber servers that do not follow the XMPP specification, which causes libpurple to connect to the server without the expected encryption and allows remote attackers to sniff sessions.
CVE-2009-3025	Unspecified vulnerability in Pidgin 2.6.0 allows remote attackers to cause a denial of service (crash) via a link in a Yahoo IM.
CVE-2009-2694	The msn_slplink_process_msg function in libpurple/protocols/msn/slplink.c in libpurple, as used in Pidgin (formerly Gaim) before 2.5.9 and Adium 1.3.5 and earlier, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) by sending multiple crafted SLP (aka MSNSLP) messages to trigger an overwrite of an arbitrary memory location. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2009-1376.
CVE-2009-1889	The OSCAR protocol implementation in Pidgin before 2.5.8 misinterprets the ICQWebMessage message type as the ICQSMS message type, which allows remote attackers to cause a denial of service (application crash) via a crafted ICQ web message that triggers allocation of a large amount of memory.
CVE-2009-1376	Multiple integer overflows in the msn_slplink_process_msg functions in the MSN protocol handler in (1) libpurple/protocols/msn/slplink.c and (2) libpurple/protocols/msnsp9/slplink.c in Pidgin (formerly Gaim) before 2.5.6 on 32-bit platforms allow remote attackers to execute arbitrary code via a malformed SLP message with a crafted offset value, leading to buffer overflows. NOTE: this issue exists because of an incomplete fix for CVE-2008-2927.
CVE-2009-1375	The PurpleCircBuffer implementation in Pidgin (formerly Gaim) before 2.5.6 does not properly maintain a certain buffer, which allows remote attackers to cause a denial of service (memory corruption and application crash) via vectors involving the (1) XMPP or (2) Sametime protocol.

CVE-2009-1374	Buffer overflow in the decrypt_out function in Pidgin (formerly Gaim) before 2.5.6 allows remote attackers to cause a denial of service (application crash) via a QQ packet.
CVE-2009-1373	Buffer overflow in the XMPP SOCKS5 bytestream server in Pidgin (formerly Gaim) before 2.5.6 allows remote authenticated users to execute arbitrary code via vectors involving an outbound XMPP file transfer. NOTE: some of these details are obtained from third party information.
CVE-2008-3532	The NSS plugin in libpurple in Pidgin 2.4.3 does not verify SSL certificates, which makes it easier for remote attackers to trick a user into accepting an invalid server certificate for a spoofed service.
CVE-2008-2927	Multiple integer overflows in the msn_slplink_process_msg functions in the MSN protocol handler in (1) libpurple/protocols/msn/slplink.c and (2) libpurple/protocols/msnp9/slplink.c in Pidgin before 2.4.3 and Adium before 1.3 allow remote attackers to execute arbitrary code via a malformed SLP message with a crafted offset value, a different vulnerability than CVE-2008-2955.
CVE-2008-2955	Pidgin 2.4.1 allows remote attackers to cause a denial of service (crash) via a long filename that contains certain characters, as demonstrated using an MSN message that triggers the crash in the msn_slplink_process_msg function.
CVE-2008-2956	** DISPUTED ** Memory leak in Pidgin 2.0.0, and possibly other versions, allows remote attackers to cause a denial of service (memory consumption) via malformed XML documents. NOTE: this issue has been disputed by the upstream vendor, who states: "I was never able to identify a scenario under which a problem occurred and the original reporter wasn't able to supply any sort of reproduction details."
CVE-2008-2957	The UPnP functionality in Pidgin 2.0.0, and possibly other versions, allows remote attackers to trigger the download of arbitrary files and cause a denial of service (memory or disk consumption) via a UDP packet that specifies an arbitrary URL.
CVE-2007-4999	libpurple in Pidgin 2.1.0 through 2.2.1, when using HTML logging, allows remote attackers to cause a denial of service (NULL dereference and application crash) via a message that contains invalid HTML data, a different vector than CVE-2007-4996.
CVE-2007-4996	libpurple in Pidgin before 2.2.1 does not properly handle MSN nudge messages from users who are not on the receiver's buddy list, which allows remote attackers to cause a denial of service (crash) via a nudge message that triggers an access of "an invalid memory location."
CVE-2007-3841	Unspecified vulnerability in Pidgin (formerly Gaim) 2.0.2 for Linux allows remote authenticated users, who are listed in a users list, to execute certain commands via unspecified vectors, aka ZD-00000035. NOTE: this information is based upon a vague advisory by a vulnerability information sales organization that does not coordinate with vendors or release actionable advisories. A CVE has been assigned for tracking purposes, but duplicates with other CVEs are difficult to determine.

## Thunderbird CVEs

cve_id	description
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-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-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-2002-2437	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 sensitive information about visited web pages by calling this method.
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-2004-0757	Heap-based buffer overflow in the SendUidl in the POP3 capability for Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, may allow remote POP3 mail servers to execute arbitrary code.
CVE-2004-0761	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote attackers to use certain redirect sequences to spoof the security lock icon that makes a web page appear to be encrypted.
CVE-2004-0762	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to install arbitrary extensions by using interactive events to manipulate the XPIInstall Security dialog box.

CVE-2004-0764	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to hijack the user interface via the "chrome" flag and XML User Interface Language (XUL) files.
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-2004-0902	Multiple heap-based buffer overflows in Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via (1) the "Send page" functionality, (2) certain responses from a malicious POP3 server, or (3) a link containing a non-ASCII hostname.
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-2004-0904	Integer overflow in the bitmap (BMP) decoder for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to execute arbitrary code via wide bitmap files that trigger heap-based buffer overflows.
CVE-2004-0906	The XPIInstall installer in Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 sets insecure permissions for certain installed files within xpi packages, which could allow local users to overwrite arbitrary files or execute arbitrary code.
CVE-2004-0907	The Linux install .tar.gz archives for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8, create certain files with insecure permissions, which could allow local users to overwrite those files and execute arbitrary code.
CVE-2004-0908	Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows untrusted Javascript code to read and write to the clipboard, and possibly obtain sensitive information, via script-generated events such as Ctrl-Ins.
CVE-2004-0909	Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 may allow remote attackers to trick users into performing unexpected actions, including installing software, via signed scripts that request enhanced abilities using the enablePrivilege parameter, then modify the meaning of certain security-relevant dialog messages.
CVE-2004-1449	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7 allows remote attackers to determine the location of files on a user's hard drive by obscuring a file upload control and tricking the user into dragging text into that control.
CVE-2004-2226	Mozilla Mail 1.7.1 and 1.7.3, and Thunderbird before 0.9, when HTML-Mails is enabled, allows remote attackers to determine valid e-mail addresses via an HTML e-mail that references a Cascading Style Sheets (CSS) document on the attacker's server.
CVE-2005-0142	Firefox 0.9, Thunderbird 0.6 and other versions before 0.9, and Mozilla 1.7 before 1.7.5 save temporary files with world-readable permissions, which allows local users to read certain web content or attachments that belong to other users, e.g. content that is managed by helper applications such as PDF.
CVE-2005-0148	Thunderbird before 0.9, when running on Windows systems, uses the default handler when processing javascript: links, which invokes Internet Explorer and may expose the Thunderbird user to vulnerabilities in the version of Internet Explorer that is installed on the user's system. NOTE: since the invocation between multiple products is a common practice, and the vulnerabilities inherent in multi-product interactions are not easily enumerable, this issue might be REJECTED in the future.
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-2005-0255	String handling functions in Mozilla 1.7.3, Firefox 1.0, and Thunderbird before 1.0.2, such as the nsTSubstring_CharT::Replace function, do not properly check the return values of other functions that resize the string, which allows remote attackers to cause a denial of service and possibly execute arbitrary code by forcing an out-of-memory state that causes a reallocation to fail and return a pointer to a fixed address, which leads to heap corruption.
CVE-2005-0399	Heap-based buffer overflow in GIF2.cpp in Firefox before 1.0.2, Mozilla before 1.7.6, and Thunderbird before 1.0.2, and possibly other applications that use the same library, allows remote attackers to execute arbitrary code via a GIF image with a crafted Netscape extension 2 block and buffer size.
CVE-2005-0590	The installation confirmation dialog in Firefox before 1.0.1, Thunderbird before 1.0.1, and Mozilla before 1.7.6 allows remote attackers to use InstallTrigger to spoof the hostname of the host performing the installation via a long "user:pass" sequence in the URL, which appears before the real hostname.
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-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-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-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-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-2006-0236	GUI display truncation vulnerability in Mozilla Thunderbird 1.0.2, 1.0.6, and 1.0.7 allows user-assisted attackers to execute arbitrary 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-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-2006-0295	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 QueryInterface method of the built-in Location and Navigator objects, which leads to memory corruption.
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-2006-0299	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-2006-0748	Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to execute arbitrary code via "an invalid and non-sensical ordering of table-related tags" that results in a negative array index.
CVE-2006-0749	nsHTMLContentSink.cpp 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) and possibly execute arbitrary code via unknown vectors involving a "particular sequence of HTML tags" that leads to memory corruption.
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-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-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-2006-1529	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1530	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1531	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1723	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.
CVE-2006-1724	Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via attack vectors related to DHTML.

CVE-2006-1725	Mozilla Firefox 1.5 before 1.5.0.2 and SeaMonkey before 1.0.1 causes certain windows to become translucent due to an interaction between XUL content windows and the history mechanism, which might allow user-assisted remote attackers to trick users into executing arbitrary code.
CVE-2006-1726	Unspecified vulnerability in Firefox and Thunderbird 1.5 before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to bypass the <code>js_ValueToFunctionObject</code> check and execute arbitrary code via unknown vectors involving <code>setTimeout</code> and Firefox' <code>ForEach</code> method.
CVE-2006-1727	Unspecified vulnerability in Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to gain chrome privileges via multiple attack vectors related to the use of XBL scripts with "Print Preview".
CVE-2006-1728	Unspecified vulnerability in Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to execute arbitrary code via unknown vectors related to the <code>crypto.generateCRMFRequest</code> method.
CVE-2006-1729	Mozilla Firefox 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to read arbitrary files by (1) inserting the target filename into a text box, then turning that box into a file upload control, or (2) changing the type of the input control that is associated with an event handler.
CVE-2006-1730	Integer overflow in Mozilla Firefox and Thunderbird 1.x before 1.5.0.2 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0.1 allows remote attackers to execute arbitrary code via a large number in the CSS letter-spacing property that leads to a heap-based buffer overflow.
CVE-2006-1731	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 returns the Object class prototype instead of the global window object when (1) <code>.valueOf.call</code> or (2) <code>.valueOf.apply</code> are called without any arguments, which allows remote attackers to conduct cross-site scripting (XSS) attacks.
CVE-2006-1732	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 bypass same-origin protections and conduct cross-site scripting (XSS) attacks via unspecified vectors involving the <code>window.controllers</code> array.
CVE-2006-1733	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 does not properly protect the compilation scope of privileged built-in XBL bindings, which allows remote attackers to execute arbitrary code via the (1) <code>valueOf.call</code> or (2) <code>valueOf.apply</code> methods of an XBL binding, or (3) "by inserting an XBL method into the DOM's <code>document.body.prototype</code> chain."
CVE-2006-1734	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 execute arbitrary code by using the <code>Object.watch</code> method to access the "clone parent" internal function.
CVE-2006-1735	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 execute arbitrary code by using an <code>eval</code> in an XBL method binding ( <code>XBL.method.eval</code> ) to create Javascript functions that are compiled with extra privileges.
CVE-2006-1736	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 trick users into downloading and saving an executable file via an image that is overlaid by a transparent image link that points to the executable, which causes the executable to be saved when the user clicks the "Save image as..." option. NOTE: this attack is made easier due to a GUI truncation issue that prevents the user from seeing the malicious extension when there is extra whitespace in the filename.
CVE-2006-1737	Integer overflow 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) and possibly execute arbitrary bytecode via JavaScript with a large regular expression.
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) <code>-moz-grid</code> and (2) <code>-moz-grid-group</code> display styles.
CVE-2006-1739	The CSS border-rendering code 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) and possibly execute arbitrary code via certain Cascading Style Sheets (CSS) that causes an out-of-bounds array write and buffer overflow.
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-2006-1741	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 inject arbitrary Javascript into other sites by (1) "using a modal alert to suspend an event handler while a new page is being loaded", (2) using <code>eval()</code> , and using certain variants involving (3) "new Script;" and (4) using <code>window.__proto__</code> to extend <code>eval</code> , aka "cross-site JavaScript injection".
CVE-2006-1742	The JavaScript engine 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 does not properly handle temporary variables that are not garbage collected, which might allow remote attackers to trigger operations on freed memory and cause memory corruption.

CVE-2006-2775	Mozilla Firefox and Thunderbird before 1.5.0.4 associates XUL attributes with the wrong URL under certain unspecified circumstances, which might allow remote attackers to bypass restrictions by causing a persisted string to be associated with the wrong URL.
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-2006-2778	The crypto.signText function in Mozilla Firefox and Thunderbird before 1.5.0.4 allows remote attackers to execute arbitrary code via certain optional Certificate Authority name arguments, which causes an invalid array index and triggers a buffer overflow.
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-2006-2780	Integer overflow in Mozilla Firefox and Thunderbird before 1.5.0.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via "jsstr tagify," which leads to memory corruption.
CVE-2006-2781	Double free vulnerability in nsVCard.cpp in Mozilla Thunderbird before 1.5.0.4 and SeaMonkey before 1.0.2 allows remote attackers to cause a denial of service (hang) and possibly execute arbitrary code via a VCard that contains invalid base64 characters.
CVE-2006-2783	Mozilla Firefox and Thunderbird before 1.5.0.4 strip the Unicode Byte-order-Mark (BOM) from a UTF-8 page before the page is passed to the parser, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a BOM sequence in the middle of a dangerous tag such as SCRIPT.
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-2006-2787	EvalInSandbox in Mozilla Firefox and Thunderbird before 1.5.0.4 allows remote attackers to gain privileges via javascript that calls the valueOf method on objects that were created outside of the sandbox.
CVE-2006-3113	Mozilla Firefox 1.5 before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via simultaneous XPCOM events, which causes a timer object to be deleted in a way that triggers memory corruption.
CVE-2006-3802	Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to hijack native DOM methods from objects in another domain and conduct cross-site scripting (XSS) attacks using DOM methods of the top-level object.
CVE-2006-3803	Race condition in the JavaScript garbage collection in Mozilla Firefox 1.5 before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 might allow remote attackers to execute arbitrary code by causing the garbage collector to delete a temporary variable while it is still being used during the creation of a new Function object.
CVE-2006-3804	Heap-based buffer overflow in Mozilla Thunderbird before 1.5.0.5 and SeaMonkey before 1.0.3 allows remote attackers to cause a denial of service (crash) via a VCard attachment with a malformed base64 field, which copies more data than expected due to an integer underflow.
CVE-2006-3805	The Javascript engine in Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 might allow remote attackers to execute arbitrary code via vectors involving garbage collection that causes deletion of a temporary object that is still being used.
CVE-2006-3806	Multiple integer overflows in the Javascript engine in Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 might allow remote attackers to execute arbitrary code via vectors involving (1) long strings in the toSource method of the Object, Array, and String objects; and (2) unspecified "string function arguments."
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-2006-3809	Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows scripts with the UniversalBrowserRead privilege to gain UniversalXPConnect privileges and possibly execute code or obtain sensitive data by reading into a privileged context.
CVE-2006-3810	Cross-site scripting (XSS) vulnerability in Mozilla Firefox 1.5 before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to inject arbitrary web script or HTML via the XPCNativeWrapper(window).Function construct.
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-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-2006-4340	Mozilla Network Security Service (NSS) library before 3.11.3, as used in Mozilla Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5, when using an RSA key with exponent 3, does not properly handle extra data in a signature, which allows remote attackers to forge signatures for SSL/TLS and email certificates, a similar vulnerability to CVE-2006-4339. NOTE: on 20061107, Mozilla released an advisory stating that these versions were not completely patched by MFSA2006-60. The newer fixes for 1.5.0.7 are covered by CVE-2006-5462.
CVE-2006-4565	Heap-based buffer overflow in Mozilla Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a JavaScript regular expression with a "minimal quantifier."
CVE-2006-4566	Mozilla Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5 allows remote attackers to cause a denial of service (crash) via a malformed JavaScript regular expression that ends with a backslash in an unterminated character set ("\\\"), which leads to a buffer over-read.
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-2006-4570	Mozilla Thunderbird before 1.5.0.7 and SeaMonkey before 1.0.5, with "Load Images" enabled, allows remote user-assisted attackers to bypass settings that disable JavaScript via a remote XBL file in a message that is loaded when the user views, forwards, or replies to the original message.
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-2006-5462	Mozilla Network Security Service (NSS) library before 3.11.3, as used in Mozilla Firefox before 1.5.0.8, Thunderbird before 1.5.0.8, and SeaMonkey before 1.0.6, when using an RSA key with exponent 3, does not properly handle extra data in a signature, which allows remote attackers to forge signatures for SSL/TLS and email certificates. NOTE: this identifier is for unpatched product versions that were originally intended to be addressed by CVE-2006-4340.
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-2006-5464	Multiple unspecified vulnerabilities in the layout 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) via unspecified vectors.
CVE-2006-5747	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 code via the XML.prototype.hasOwnProperty JavaScript function.
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-2006-6497	Multiple unspecified vulnerabilities in the layout engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown attack vectors.
CVE-2006-6498	Multiple unspecified vulnerabilities in the JavaScript engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, SeaMonkey before 1.0.7, and Mozilla 1.7 and probably earlier on Solaris, allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown impact and attack vectors.
CVE-2006-6499	The js_dtoa function in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 overwrites memory instead of exiting when the floating point precision is reduced, which allows remote attackers to cause a denial of service via any plugins that reduce the precision.
CVE-2006-6500	Heap-based buffer overflow in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by setting the CSS cursor to certain images that cause an incorrect size calculation when converting to a Windows bitmap.
CVE-2006-6501	Unspecified vulnerability in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to gain privileges and install malicious code via the watch Javascript function.
CVE-2006-6502	Use-after-free vulnerability in the LiveConnect bridge code for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to cause a denial of service (crash) via unknown vectors.

CVE-2006-6503	Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to bypass cross-site scripting (XSS) protection by changing the src attribute of an IMG element to a javascript: URI.
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-2006-6505	Multiple heap-based buffer overflows in Mozilla Thunderbird before 1.5.0.9 and SeaMonkey before 1.0.7 allow remote attackers to execute arbitrary code via (1) external message bodies with long Content-Type headers or (2) long RFC2047-encoded (MIME non-ASCII) headers.
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-2007-0009	Stack-based buffer overflow 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, Thunderbird before 1.5.0.10, SeaMonkey before 1.0.8, and certain Sun Java System server products before 20070611, allows remote attackers to execute arbitrary code via invalid "Client Master Key" length values.
CVE-2007-0775	Multiple unspecified vulnerabilities in the layout 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 allow remote attackers to cause a denial of service (crash) and potentially execute arbitrary code via certain vectors.
CVE-2007-0776	Heap-based buffer overflow in the _cairo_pen_init function in Mozilla Firefox 2.x before 2.0.0.2, Thunderbird before 1.5.0.10, and SeaMonkey before 1.0.8 allows remote attackers to execute arbitrary code via a large stroke-width attribute in the clipPath element in an SVG file.
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-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-2007-2867	Multiple vulnerabilities in the layout 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) via vectors related to dangling pointers, heap corruption, signed/unsigned, and other issues.
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-2007-3734	Multiple unspecified vulnerabilities in the browser 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-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-2007-3844	Mozilla Firefox 2.0.0.5, Thunderbird 2.0.0.5 and before 1.5.0.13, and SeaMonkey 1.1.3 allows remote attackers to conduct cross-site scripting (XSS) attacks with chrome privileges via an addon that inserts a (1) javascript: or (2) data: link into an about:blank document loaded by chrome via (a) the window.open function or (b) a content.location assignment, aka "Cross Context Scripting." NOTE: this issue is caused by a CVE-2007-3089 regression.
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-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-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-2007-5339	Multiple vulnerabilities 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 or assert errors.
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-2008-0304	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-2008-0412	The browser engine in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via vectors related to the (1) nsTableFrame::GetFrameAtOrBefore, (2) nsAccessibilityService::GetAccessible, (3) nsBindingManager::GetNestedInsertionPoint, (4) nsXBLPrototypeBinding::AttributeChanged, (5) nsColumnSetFrame::GetContentInsertionFrame, and (6) nsLineLayout::TrimTrailingWhiteSpaceIn methods, and other vectors.
CVE-2008-0413	The JavaScript engine in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via (1) a large switch statement, (2) certain uses of watch and eval, (3) certain uses of the mousedown event listener, and other vectors.
CVE-2008-0415	Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allows remote attackers to execute script outside of the sandbox and conduct cross-site scripting (XSS) attacks via multiple vectors including the XMLHttpRequest.load function, aka "JavaScript privilege escalation bugs."
CVE-2008-0416	Multiple cross-site scripting (XSS) vulnerabilities in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 allow remote attackers to inject arbitrary web script or HTML via certain character encodings, including (1) a backspace character that is treated as whitespace, (2) 0x80 with Shift_JIS encoding, and (3) "zero-length non-ASCII sequences" in certain Asian character sets.
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-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-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-2008-1233	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 "XPCNativeWrapper pollution."
CVE-2008-1234	Cross-site scripting (XSS) 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 inject arbitrary web script or HTML via event handlers, aka "Universal XSS using event handlers."
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-2008-1236	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors related to the layout engine.
CVE-2008-1237	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors related to the JavaScript engine.
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-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-2008-2798	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via unknown vectors related to the layout engine.
CVE-2008-2799	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via unknown vectors related to the JavaScript engine.
CVE-2008-2802	Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 allow remote attackers to execute arbitrary code via an XUL document that includes a script from a chrome: URI that points to a fastload file, related to this file's "privilege level."
CVE-2008-2803	The mozIJSSubScriptLoader.LoadScript function in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 does not apply XPCNativeWrappers to scripts loaded from (1) file: URIs, (2) data: URIs, or (3) certain non-canonical chrome: URIs, which allows remote attackers to execute arbitrary code via vectors involving third-party add-ons.
CVE-2008-2806	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 on Mac OS X allow remote attackers to bypass the Same Origin Policy and create arbitrary socket connections via a crafted Java applet, related to the Java Embedding Plugin (JEP) and Java LiveConnect.
CVE-2008-2808	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 do not properly escape HTML in file:// URLs in directory listings, which allows remote attackers to conduct cross-site scripting (XSS) attacks or have unspecified other impact via a crafted filename.
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-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-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-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-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-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 NPOObject in the nsNPObjWrapper::GetNewOrUsed function in nsJSNPRuntime.cpp.
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-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-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-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-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-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-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-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-2008-5018	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2009-0652	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-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-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-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-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-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-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-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-2009-1302	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-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-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-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 JSOPROP_PERMANENT attribute.
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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2009-3983	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2010-1199	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.
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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2010-2769	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 added to a document in which the designMode property is enabled.
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-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-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-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-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-2010-3169	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-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-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-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-2010-3175	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-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-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-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-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-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-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-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-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-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-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-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-2010-3777	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-2010-3778	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-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-2011-0053	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-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-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-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-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-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-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-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-2011-0074, CVE-2011-0077, and CVE-2011-0078.
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-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-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-2011-0080	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2011-2377	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-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-2011-2605	CRLF injection vulnerability in the nsCookieService::SetCookieStringInternal function in network/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-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-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-2011-2982	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-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-2011-2984	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2011-3647	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-2011-3648	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-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-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-2011-3651	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 7.0 and Thunderbird 7.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
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-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-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-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-2011-3658	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 unspecified other impact via vectors involving removal of SVG elements.
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-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-2011-3661	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-2011-3663	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-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-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-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-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-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-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-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-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-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-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-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-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-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-2012-0451	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-2012-0452	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-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-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-2012-0456	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-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-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-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-2012-0460	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-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-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-2012-0463	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-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-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-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-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-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-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-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-2012-0473	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-2012-0474	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-2012-0475	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-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-2012-0478	The texImage2D implementation in the WebGL subsystem 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 does not properly restrict JSVAL_TO_OBJECT casts, which might allow remote attackers to execute arbitrary code via a crafted web page.
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-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.
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-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-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-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-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 wsocck32.dll file in an application directory.
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-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-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-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-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-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-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-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-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-2012-1954	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-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-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-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-2012-1958	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-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-2012-1960	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-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-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-2012-1963	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 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-2012-1964	The certificate-warning functionality in browser/components/certerror/content/aboutCertError.xhtml in Mozilla Firefox 4.x through 12.0, 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-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-2012-1970	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-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-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-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-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-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-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-2012-3105	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-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-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-2012-3958	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-2012-3959	Use-after-free vulnerability in the nsRangeUpdater::SelAdjDeleteNode 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-2012-3960	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-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-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-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-2012-3964	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-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-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-2012-3968	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-2012-3969	Integer overflow in the nsSVGFE>MorphologyElement::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-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-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-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-2012-3974	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-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-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-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-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-2012-3982	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-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-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-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-2012-3986	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-2012-3988	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-2012-3989	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-2012-3990	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-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-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-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-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-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-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-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-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-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-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-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-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-2012-4186	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-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-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-2012-4191	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-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-2012-4193	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-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-2012-4195	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-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-2012-4201	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-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-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-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-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-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-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-2012-4212	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-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-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-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-2012-4216	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-2012-4217	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-2012-4218	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-2012-5354	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-2012-5829	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2013-0754	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-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-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-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-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-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-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-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-2013-0762	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-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-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-2013-0765	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-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-2013-0767	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-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-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-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-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-2013-0772	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-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-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-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-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-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-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-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-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-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-2013-0782	Heap-based buffer overflow in the nsSaveAsCharset::DoCharsetConversion 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 unspecified vectors.
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-2013-0784	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-2013-0787	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-2013-0788	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-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-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-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-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-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-2013-0799	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-2013-0800	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-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-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-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-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-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-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-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-2013-1678	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 operation) via unspecified 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-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-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-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-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-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-2013-1686	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-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-2013-1690	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-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-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-2013-1694	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-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) <code>toString</code> or (2) <code>valueOf</code> method.
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-2013-1706	Stack-based buffer overflow in <code>maintenanceservice.exe</code> 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-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-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-2013-1710	The <code>crypto.generateCRMFRequest</code> 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-2013-1712	Multiple untrusted search path vulnerabilities in <code>updater.exe</code> 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-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-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-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-2013-1718	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-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-2013-1720	The <code>nsHtml5TreeBuilder::resetTheInsertionMode</code> 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-2013-1722	Use-after-free vulnerability in the <code>nsAnimationManager::BuildAnimations</code> 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-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-2013-1724	Use-after-free vulnerability in the <code>mozilla::dom::HTMLFormElement::IsDefaultSubmitElement</code> 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-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-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-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-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-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-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-2013-1736	The nsGfxScrollViewInner::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-2013-1737	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-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-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-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-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-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-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-2013-5597	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-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-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-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-2013-5602	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-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-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-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-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-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-2013-5616	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-2013-5618	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-2013-6671	The nsGfxScrollViewInner::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-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-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-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-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-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-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-2014-1486	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-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-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-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-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-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-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-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-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-2014-1509	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 that renders fonts in a PDF document.
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-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-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-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-2014-1514	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 code or cause a denial of service (out-of-bounds write and application crash) by triggering incorrect use of the TypedArrayObject class.
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-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-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-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-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-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-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-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-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-2014-1541	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 service (heap memory corruption) via crafted web content.
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-2014-1547	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2014-1567	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-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-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-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-2014-1578	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-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-2014-1585	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-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-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-2014-1590	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-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-2014-1593	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-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-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-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-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-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-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-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-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-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-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-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-2015-0816	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 Same Origin Policy, as demonstrated by the resource: URL associated with PDF.js.
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-2015-0827	Heap-based buffer overflow in the mozilla::gfx::CopyRect function in Mozilla Firefox before 36.0, Firefox ESR 31.x before 31.5, and Thunderbird before 31.5 allows remote attackers to obtain sensitive information from uninitialized process memory via a malformed SVG graphic.
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-2015-0833	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 DLL in (1) the current working directory or (2) a temporary directory, as demonstrated by bcrypt.dll.
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-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-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-2015-2713	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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-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-2016-1952	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-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-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-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-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-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-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-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-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.

## WordPress CVEs

cve_id	description
CVE-2014-5266	The Incutio XML-RPC (IXR) Library, as used in WordPress before 3.9.2 and Drupal 6.x before 6.33 and 7.x before 7.31, does not limit the number of elements in an XML document, which allows remote attackers to cause a denial of service (CPU consumption) via a large document, a different vulnerability than CVE-2014-5265.
CVE-2014-5265	The Incutio XML-RPC (IXR) Library, as used in WordPress before 3.9.2 and Drupal 6.x before 6.33 and 7.x before 7.31, permits entity declarations without considering recursion during entity expansion, which allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.
CVE-2015-5734	Cross-site scripting (XSS) vulnerability in the legacy theme preview implementation in wp-includes/theme.php in WordPress before 4.2.4 allows remote attackers to inject arbitrary web script or HTML via a crafted string.
CVE-2015-5733	Cross-site scripting (XSS) vulnerability in the refreshAdvancedAccessibilityOfItem function in wp-admin/js/nav-menu.js in WordPress before 4.2.4 allows remote attackers to inject arbitrary web script or HTML via an accessibility-helper title.
CVE-2015-5732	Cross-site scripting (XSS) vulnerability in the form function in the WP_Nav_Menu_Widget class in wp-includes/default-widgets.php in WordPress before 4.2.4 allows remote attackers to inject arbitrary web script or HTML via a widget title.
CVE-2015-5731	Cross-site request forgery (CSRF) vulnerability in wp-admin/post.php in WordPress before 4.2.4 allows remote attackers to hijack the authentication of administrators for requests that lock a post, and consequently cause a denial of service (editing blockage), via a get-post-lock action.

CVE-2015-5730	The sanitize_widget_instance function in wp-includes/class-wp-customize-widgets.php in WordPress before 4.2.4 does not use a constant-time comparison for widgets, which allows remote attackers to conduct a timing side-channel attack by measuring the delay before inequality is calculated.
CVE-2015-2213	SQL injection vulnerability in the wp_untrash_post_comments function in wp-includes/post.php in WordPress before 4.2.4 allows remote attackers to execute arbitrary SQL commands via a comment that is mishandled after retrieval from the trash.
CVE-2015-3439	Cross-site scripting (XSS) vulnerability in the Ephox (formerly Moxiecode) plupload.flash.swf shim 2.1.2 in Plupload, as used in WordPress 3.9.x, 4.0.x, and 4.1.x before 4.1.2 and other products, allows remote attackers to execute same-origin JavaScript functions via the target parameter, as demonstrated by executing a certain click function, related to _init.as and _fireEvent.as.
CVE-2015-3438	Multiple cross-site scripting (XSS) vulnerabilities in WordPress before 4.1.2, when MySQL is used without strict mode, allow remote attackers to inject arbitrary web script or HTML via a (1) four-byte UTF-8 character or (2) invalid character that reaches the database layer, as demonstrated by a crafted character in a comment.
CVE-2015-5623	WordPress before 4.2.3 does not properly verify the edit_posts capability, which allows remote authenticated users to bypass intended access restrictions and create drafts by leveraging the Subscriber role, as demonstrated by a post-quickdraft-save action to wp-admin/post.php.
CVE-2015-5622	Cross-site scripting (XSS) vulnerability in WordPress before 4.2.3 allows remote authenticated users to inject arbitrary web script or HTML by leveraging the Author or Contributor role to place a crafted shortcode inside an HTML element, related to wp-includes/kses.php and wp-includes/shortcodes.php.
CVE-2015-3440	Cross-site scripting (XSS) vulnerability in wp-includes/wp-db.php in WordPress before 4.2.1 allows remote attackers to inject arbitrary web script or HTML via a long comment that is improperly stored because of limitations on the MySQL TEXT data type.
CVE-2015-3429	Cross-site scripting (XSS) vulnerability in example.html in Genericons before 3.3.1, as used in WordPress before 4.2.2, allows remote attackers to inject arbitrary web script or HTML via a fragment identifier.
CVE-2014-9039	wp-login.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 might allow remote attackers to reset passwords by leveraging access to an e-mail account that received a password-reset message.
CVE-2014-9038	wp-includes/http.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to conduct server-side request forgery (SSRF) attacks by referring to a 127.0.0.0/8 resource.
CVE-2014-9037	WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 might allow remote attackers to obtain access to an account idle since 2008 by leveraging an improper PHP dynamic type comparison for an MD5 hash.
CVE-2014-9036	Cross-site scripting (XSS) vulnerability in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to inject arbitrary web script or HTML via a crafted Cascading Style Sheets (CSS) token sequence in a post.
CVE-2014-9035	Cross-site scripting (XSS) vulnerability in Press This in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2014-9034	wp-includes/class-phpass.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows remote attackers to cause a denial of service (CPU consumption) via a long password that is improperly handled during hashing, a similar issue to CVE-2014-9016.
CVE-2014-9033	Cross-site request forgery (CSRF) vulnerability in wp-login.php in WordPress 3.7.4, 3.8.4, 3.9.2, and 4.0 allows remote attackers to hijack the authentication of arbitrary users for requests that reset passwords.
CVE-2014-9032	Cross-site scripting (XSS) vulnerability in the media-playlists feature in WordPress before 3.9.x before 3.9.3 and 4.x before 4.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2014-9031	Cross-site scripting (XSS) vulnerability in the wptexturize function in WordPress before 3.7.5, 3.8.x before 3.8.5, and 3.9.x before 3.9.3 allows remote attackers to inject arbitrary web script or HTML via crafted use of shortcode brackets in a text field, as demonstrated by a comment or a post.
CVE-2003-1599	PHP remote file inclusion vulnerability in wp-links/links.all.php in WordPress 0.70 allows remote attackers to execute arbitrary PHP code via a URL in the \$abspath variable.
CVE-2003-1598	SQL injection vulnerability in log.header.php in WordPress 0.7 and earlier allows remote attackers to execute arbitrary SQL commands via the posts variable.
CVE-2014-5240	Cross-site scripting (XSS) vulnerability in wp-includes/pluggable.php in WordPress before 3.9.2, when Multisite is enabled, allows remote authenticated administrators to inject arbitrary web script or HTML, and obtain Super Admin privileges, via a crafted avatar URL.
CVE-2014-5205	wp-includes/pluggable.php in WordPress before 3.9.2 does not use delimiters during concatenation of action values and uid values in CSRF tokens, which makes it easier for remote attackers to bypass a CSRF protection mechanism via a brute-force attack.
CVE-2014-5204	wp-includes/pluggable.php in WordPress before 3.9.2 rejects invalid CSRF nonces with a different timing depending on which characters in the nonce are incorrect, which makes it easier for remote attackers to bypass a CSRF protection mechanism via a brute-force attack.

CVE-2014-5203	wp-includes/class-wp-customize-widgets.php in the widget implementation in WordPress 3.9.x before 3.9.2 might allow remote attackers to execute arbitrary code via crafted serialized data.
CVE-2014-4534	Multiple cross-site scripting (XSS) vulnerabilities in videoplayer/autoload.php in the HTML5 Video Player with Playlist plugin 2.4.0 and earlier for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) theme or (2) playlistmod parameter.
CVE-2014-4603	Multiple cross-site scripting (XSS) vulnerabilities in yupdates_application.php in the Yahoo! Updates for WordPress plugin 1.0 and earlier for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) secret, (2) key, or (3) appid parameter.
CVE-2014-4600	Multiple cross-site scripting (XSS) vulnerabilities in contact/edit.php in the WP Ultimate Email Marketer plugin 1.1.0 and earlier for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) listname or (2) contact parameter.
CVE-2014-4529	Cross-site scripting (XSS) vulnerability in fpg_preview.php in the Flash Photo Gallery plugin 0.7 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the path parameter.
CVE-2012-4915	Directory traversal vulnerability in the Google Doc Embedder plugin before 2.5.4 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter to libs/pdf.php.
CVE-2014-3845	Cross-site request forgery (CSRF) vulnerability in the TinyMCE Color Picker plugin before 1.2 for WordPress allows remote attackers to hijack the authentication of unspecified users for requests that change plugin settings via unknown vectors. NOTE: some of these details are obtained from third party information.
CVE-2014-3844	The TinyMCE Color Picker plugin before 1.2 for WordPress does not properly check permissions, which allows remote attackers to modify plugin settings via unspecified vectors. NOTE: some of these details are obtained from third party information.
CVE-2014-3843	Cross-site request forgery (CSRF) vulnerability in the Search Everything plugin before 8.1.1 for WordPress allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.
CVE-2014-3841	Cross-site scripting (XSS) vulnerability in the Contact Bank plugin before 2.0.20 for WordPress allows remote attackers to inject arbitrary web script or HTML via the Label field, related to form layout configuration. NOTE: some of these details are obtained from third party information.
CVE-2014-3210	SQL injection vulnerability in dopbs-backend-forms.php in the Booking System (Booking Calendar) plugin before 1.3 for WordPress allows remote authenticated users to execute arbitrary SQL commands via the booking_form_id parameter to wp-admin/admin-ajax.php.
CVE-2013-2706	Cross-site request forgery (CSRF) vulnerability in the Stream Video Player plugin 1.4.0 for WordPress allows remote attackers to hijack the authentication of administrators for requests that change plugin settings via unspecified vectors.
CVE-2014-0166	The wp_validate_auth_cookie function in wp-includes/pluggable.php in WordPress before 3.7.2 and 3.8.x before 3.8.2 does not properly determine the validity of authentication cookies, which makes it easier for remote attackers to obtain access via a forged cookie.
CVE-2014-0165	WordPress before 3.7.2 and 3.8.x before 3.8.2 allows remote authenticated users to publish posts by leveraging the Contributor role, related to wp-admin/includes/post.php and wp-admin/includes/class-wp-posts-list-table.php.
CVE-2012-4920	Directory traversal vulnerability in the zing_forum_output function in forum.php in the Zingiri Forum (aka Forums) plugin before 1.4.4 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the url parameter to index.php.
CVE-2013-0735	Multiple SQL injection vulnerabilities in wpf.class.php in the Mingle Forum plugin before 1.0.34 for WordPress allow remote attackers to execute arbitrary SQL commands via the id parameter in a viewtopic (1) remove_post, (2) sticky, or (3) closed action or (4) thread parameter in a postreply action to index.php.
CVE-2013-0734	Multiple cross-site scripting (XSS) vulnerabilities in the Mingle Forum plugin before 1.0.34 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) search_words parameter in a search action to wpf.class.php or (2) togroupusers parameter in an add_user_togroup action to fs-admin/fs-admin.php.
CVE-2014-2265	Rock Lobster Contact Form 7 before 3.7.2 allows remote attackers to bypass the CAPTCHA protection mechanism and submit arbitrary form data by omitting the _wpcf7_captcha_challenge-719 parameter.
CVE-2014-2316	SQL injection vulnerability in se_search_default in the Search Everything plugin before 7.0.3 for WordPress allows remote attackers to execute arbitrary SQL commands via the s parameter to index.php. NOTE: some of these details are obtained from third party information.
CVE-2014-2315	Multiple cross-site scripting (XSS) vulnerabilities in the Thank You Counter Button plugin 1.8.7 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) thanks_caption, (2) thanks_caption_style, or (3) thanks_style parameter to wp-admin/options.php.
CVE-2014-1907	Multiple directory traversal vulnerabilities in the VideoWhisper Live Streaming Integration plugin before 4.29.5 for WordPress allow remote attackers to (1) read arbitrary files via a .. (dot dot) in the s parameter to ls/rtmp_login.php or (2) delete arbitrary files via a .. (dot dot) in the s parameter to ls/rtmp_logout.php.
CVE-2013-3487	Multiple cross-site scripting (XSS) vulnerabilities in the security log in the BulletProof Security plugin before .49 for WordPress allow remote attackers to inject arbitrary web script or HTML via unspecified HTML header fields to (1) 400.php, (2) 403.php, or (3) 403.php.

CVE-2013-1409	Cross-site scripting (XSS) vulnerability in the CommentLuv plugin before 2.92.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the <code>_ajax_nonce</code> parameter to <code>wp-admin/admin-ajax.php</code> .
CVE-2014-1888	Cross-site scripting (XSS) vulnerability in the BuddyPress plugin before 1.9.2 for WordPress allows remote authenticated users to inject arbitrary web script or HTML via the name field to <code>groups/create/step/group-details</code> . NOTE: this can be exploited without authentication by leveraging CVE-2014-1889.
CVE-2012-6635	<code>wp-admin/includes/class-wp-posts-list-table.php</code> in WordPress before 3.3.3 does not properly restrict excerpt-view access, which allows remote authenticated users to obtain sensitive information by visiting a draft.
CVE-2012-6634	<code>wp-admin/media-upload.php</code> in WordPress before 3.3.3 allows remote attackers to obtain sensitive information or bypass intended media-attachment restrictions via a <code>post_id</code> value.
CVE-2012-6633	Cross-site scripting (XSS) vulnerability in <code>wp-includes/default-filters.php</code> in WordPress before 3.3.3 allows remote attackers to inject arbitrary web script or HTML via an editable slug field.
CVE-2011-5270	<code>wp-admin/press-this.php</code> in WordPress before 3.0.6 does not enforce the <code>publish_posts</code> capability requirement, which allows remote authenticated users to perform publish actions by leveraging the Contributor role.
CVE-2010-5297	WordPress before 3.0.1, when a Multisite installation is used, permanently retains the "site administrators can add users" option once changed, which might allow remote authenticated administrators to bypass intended access restrictions in opportunistic circumstances via an add action after a temporary change.
CVE-2010-5296	<code>wp-includes/capabilities.php</code> in WordPress before 3.0.2, when a Multisite configuration is used, does not require the Super Admin role for the <code>delete_users</code> capability, which allows remote authenticated administrators to bypass intended access restrictions via a delete action.
CVE-2010-5295	Cross-site scripting (XSS) vulnerability in <code>wp-admin/plugins.php</code> in WordPress before 3.0.2 might allow remote attackers to inject arbitrary web script or HTML via a plugin's author field, which is not properly handled during a Delete Plugin action.
CVE-2010-5294	Multiple cross-site scripting (XSS) vulnerabilities in the <code>request_filesystem_credentials</code> function in <code>wp-admin/includes/file.php</code> in WordPress before 3.0.2 allow remote servers to inject arbitrary web script or HTML by providing a crafted error message for a (1) FTP or (2) SSH connection attempt.
CVE-2010-5293	<code>wp-includes/comment.php</code> in WordPress before 3.0.2 does not properly whitelist trackbacks and pingbacks in the blogroll, which allows remote attackers to bypass intended spam restrictions via a crafted URL, as demonstrated by a URL that triggers a substring match.
CVE-2014-1232	Cross-site scripting (XSS) vulnerability in the Foliopress WYSIWYG plugin before 2.6.8.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-7279	Cross-site scripting (XSS) vulnerability in <code>views/video-management/preview_video.php</code> in the S3 Video plugin before 0.983 for WordPress allows remote attackers to inject arbitrary web script or HTML via the <code>base</code> parameter.
CVE-2013-7276	Cross-site scripting (XSS) vulnerability in <code>inc/raf_form.php</code> in the Recommend to a friend plugin 2.0.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the <code>current_url</code> parameter.
CVE-2013-7240	Directory traversal vulnerability in <code>download-file.php</code> in the Advanced Dewplayer plugin 1.2 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the <code>dew_file</code> parameter.
CVE-2013-6993	Cross-site scripting (XSS) vulnerability in the Ad-minister plugin 0.6 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the <code>key</code> parameter in a delete action to <code>wp-admin/tools.php</code> .
CVE-2013-6992	Cross-site request forgery (CSRF) vulnerability in <code>askapache-firefox-adsense.php</code> in the AskApache Firefox Adsense plugin 3.0 and earlier for WordPress allows remote attackers to hijack the authentication of administrators for requests that conduct cross-site scripting (XSS) attacks via the <code>aafireadcode</code> parameter to <code>wp-admin/options-general.php</code> .
CVE-2013-6991	Cross-site scripting (XSS) vulnerability in the WP-Cron Dashboard plugin 1.1.5 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the <code>procname</code> parameter to <code>wp-admin/tools.php</code> .
CVE-2013-7233	Cross-site request forgery (CSRF) vulnerability in the retrospam component in <code>wp-admin/options-discussion.php</code> in WordPress 2.0.11 and earlier allows remote attackers to hijack the authentication of administrators for requests that move comments to the moderation list.
CVE-2013-0736	Multiple cross-site request forgery (CSRF) vulnerabilities in the Mingle Forum plugin 1.0.34 and possibly earlier for WordPress allow remote attackers to hijack the authentication of administrators for requests that (1) modify user privileges or (2) conduct cross-site scripting (XSS) attacks via unspecified vectors.
CVE-2013-6010	Cross-site scripting (XSS) vulnerability in the Comment Attachment plugin 1.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via the "Attachment field title."
CVE-2013-5963	Unrestricted file upload vulnerability in <code>multi.php</code> in Simple Dropbox Upload plugin before 1.8.8.1 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in <code>wp-content/uploads/wpdb/</code> .
CVE-2013-5961	Unrestricted file upload vulnerability in <code>lazyseo.php</code> in the Lazy SEO plugin 1.1.9 for WordPress allows remote attackers to execute arbitrary PHP code by uploading a PHP file, then accessing it via a direct request to the file in <code>lazy-seo/</code> .
CVE-2013-4626	Cross-site scripting (XSS) vulnerability in the BackWPup plugin before 3.0.13 for WordPress allows remote attackers to inject arbitrary web script or HTML via the <code>tab</code> parameter to <code>wp-admin/admin.php</code> .

CVE-2013-5918	Cross-site scripting (XSS) vulnerability in platinum_seo_pack.php in the Platinum SEO plugin before 1.3.8 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2013-5917	SQL injection vulnerability in wp-comments-post.php in the NOSpam PTI plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the comment_post_ID parameter.
CVE-2013-5739	The default configuration of WordPress before 3.6.1 does not prevent uploads of .swf and .exe files, which might make it easier for remote authenticated users to conduct cross-site scripting (XSS) attacks via a crafted file, related to the get_allowed_mime_types function in wp-includes/functions.php.
CVE-2013-5738	The get_allowed_mime_types function in wp-includes/functions.php in WordPress before 3.6.1 does not require the unfiltered_html capability for uploads of .htm and .html files, which might make it easier for remote authenticated users to conduct cross-site scripting (XSS) attacks via a crafted file.
CVE-2013-4340	wp-admin/includes/post.php in WordPress before 3.6.1 allows remote authenticated users to spoof the authorship of a post by leveraging the Author role and providing a modified user_ID parameter.
CVE-2013-4339	WordPress before 3.6.1 does not properly validate URLs before use in an HTTP redirect, which allows remote attackers to bypass intended redirection restrictions via a crafted string.
CVE-2013-4338	wp-includes/functions.php in WordPress before 3.6.1 does not properly determine whether data has been serialized, which allows remote attackers to execute arbitrary code by triggering erroneous PHP unserialize operations.
CVE-2013-5673	SQL injection vulnerability in testimonial.php in the IndiaNIC Testimonial plugin 2.2 for WordPress allows remote attackers to execute arbitrary SQL commands via the custom_query parameter in a testimonial_add action to wp-admin/admin-ajax.php.
CVE-2013-5672	Multiple cross-site request forgery (CSRF) vulnerabilities in the IndiaNIC Testimonial plugin 2.2 for WordPress allow remote attackers to hijack the authentication of administrators for requests that (1) add a testimonial via an iNIC_testimonial_save action; (2) add a listing template via an iNIC_testimonial_save_listing_template action; (3) add a widget template via an iNIC_testimonial_save_widget action; insert cross-site scripting (XSS) sequences via the (4) project_name, (5) project_url, (6) client_name, (7) client_city, (8) client_state, (9) description, (10) tags, (11) video_url, or (12) is_featured, (13) title, (14) widget_title, (15) no_of_testimonials, (16) filter_by_country, (17) filter_by_tags, or (18) widget_template parameter to wp-admin/admin-ajax.php.
CVE-2013-5714	Multiple cross-site scripting (XSS) vulnerabilities in ls/htmlchat.php in the VideoWhisper Live Streaming Integration plugin 4.25.3 and possibly earlier for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) name or (2) message parameter. NOTE: some of these details are obtained from third party information.
CVE-2013-3479	Cross-site request forgery (CSRF) vulnerability in the ShareThis plugin before 7.0.6 for WordPress allows remote attackers to hijack the authentication of administrators for requests that modify this plugin's settings.
CVE-2013-5098	Cross-site scripting (XSS) vulnerability in admin/admin.php in the Download Monitor plugin before 3.3.6.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the sort parameter, a different vulnerability than CVE-2013-3262.
CVE-2013-4625	Cross-site scripting (XSS) vulnerability in files/installer.cleanup.php in the Duplicator plugin before 0.4.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the package parameter.
CVE-2013-3262	Cross-site scripting (XSS) vulnerability in admin/admin.php in the Download Monitor plugin before 3.3.6.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the p parameter.
CVE-2013-3253	Cross-site request forgery (CSRF) vulnerability in admin/setting.php in the Xhanch - My Twitter plugin before 2.7.7 for WordPress allows remote attackers to hijack the authentication of administrators for requests that change unspecified settings.
CVE-2013-3256	Cross-site request forgery (CSRF) vulnerability in the Shareaholic SexyBookmarks plugin 6.1.4.0 for WordPress allows remote attackers to hijack the authentication of users for requests that "manipulate plugin settings."
CVE-2013-4954	Multiple cross-site scripting (XSS) vulnerabilities in wp-login.php in the Genetech Solutions Pie-Register plugin before 1.31 for WordPress, when "Allow New Registrations to set their own Password" is enabled, allow remote attackers to inject arbitrary web script or HTML via the (1) pass1 or (2) pass2 parameter in a register action. NOTE: some of these details are obtained from third party information.
CVE-2013-4944	Cross-site scripting (XSS) vulnerability in the BuddyPress Extended Friendship Request plugin before 1.0.2 for WordPress, when the "Friend Connections" component is enabled, allows remote attackers to inject arbitrary web script or HTML via the friendship_request_message parameter to wp-admin/admin-ajax.php. NOTE: some of these details are obtained from third party information.
CVE-2012-3414	Cross-site scripting (XSS) vulnerability in swfupload.swf in SWFUpload 2.2.0.1 and earlier, as used in WordPress before 3.3.2, TinyMCE Image Manager 1.1, and other products, allows remote attackers to inject arbitrary web script or HTML via the movieName parameter, related to the "ExternalInterface.call" function.
CVE-2013-4117	Cross-site scripting (XSS) vulnerability in includes/CatGridPost.php in the Category Grid View Gallery plugin 2.3.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the ID parameter.
CVE-2013-3491	Multiple cross-site request forgery (CSRF) vulnerabilities in the Sharebar plugin 1.2.5 for WordPress allow remote attackers to hijack the authentication of administrators for requests that (1) add or (2) modify buttons, or (3) insert cross-site scripting (XSS) sequences.

CVE-2013-2704	Cross-site request forgery (CSRF) vulnerability in the Dropdown Menu Widget plugin 1.9.1 for WordPress allows remote attackers to hijack the authentication of arbitrary users for requests that insert cross-site scripting (XSS) sequences.
CVE-2013-2205	The default configuration of SWFUpload in WordPress before 3.5.2 has an unrestrictive security.allowDomain setting, which allows remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via a crafted web site.
CVE-2013-2204	moxieplayer.as in Moxiecode moxieplayer, as used in the TinyMCE Media plugin in WordPress before 3.5.2 and other products, does not consider the presence of a # (pound sign) character during extraction of the QUERY_STRING, which allows remote attackers to pass arbitrary parameters to a Flash application, and conduct content-spoofing attacks, via a crafted string after a ? (question mark) character.
CVE-2013-2203	WordPress before 3.5.2, when the uploads directory forbids write access, allows remote attackers to obtain sensitive information via an invalid upload request, which reveals the absolute path in an XMLHttpRequest error message.
CVE-2013-2202	WordPress before 3.5.2 allows remote attackers to read arbitrary files via an oEmbed XML provider response containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.
CVE-2013-2201	Multiple cross-site scripting (XSS) vulnerabilities in WordPress before 3.5.2 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) uploads of media files, (2) editing of media files, (3) installation of plugins, (4) updates to plugins, (5) installation of themes, or (6) updates to themes.
CVE-2013-2200	WordPress before 3.5.2 does not properly check the capabilities of roles, which allows remote authenticated users to bypass intended restrictions on publishing and authorship reassignment via unspecified vectors.
CVE-2013-2199	The HTTP API in WordPress before 3.5.2 allows remote attackers to send HTTP requests to intranet servers via unspecified vectors, related to a Server-Side Request Forgery (SSRF) issue, a similar vulnerability to CVE-2013-0235.
CVE-2013-0237	Cross-site scripting (XSS) vulnerability in Plupload.as in Moxiecode plupload before 1.5.5, as used in WordPress before 3.5.1 and other products, allows remote attackers to inject arbitrary web script or HTML via the id parameter.
CVE-2013-0236	Multiple cross-site scripting (XSS) vulnerabilities in WordPress before 3.5.1 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) gallery shortcodes or (2) the content of a post.
CVE-2013-0235	The XMLRPC API in WordPress before 3.5.1 allows remote attackers to send HTTP requests to intranet servers, and conduct port-scanning attacks, by specifying a crafted source URL for a pingback, related to a Server-Side Request Forgery (SSRF) issue.
CVE-2013-2173	wp-includes/class-phpass.php in WordPress 3.5.1, when a password-protected post exists, allows remote attackers to cause a denial of service (CPU consumption) via a crafted value of a certain wp-postpass cookie.
CVE-2013-3261	Cross-site scripting (XSS) vulnerability in wp-admin/admin.php in the GRAND FLAGallery plugin before 2.72 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter in a flag-manage-gallery action.
CVE-2013-3720	Cross-site scripting (XSS) vulnerability in widget_remove.php in the Feedweb plugin before 1.9 for WordPress allows remote authenticated administrators to inject arbitrary web script or HTML via the wp_post_id parameter.
CVE-2013-3532	SQL injection vulnerability in settings.php in the Web Dorado Spider Video Player plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the theme parameter.
CVE-2013-3530	SQL injection vulnerability in playlist.php in the Spiffy XSPF Player plugin 0.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the playlist_id parameter.
CVE-2013-3529	Multiple cross-site scripting (XSS) vulnerabilities in user/obits.php in the WP FuneralPress plugin before 1.1.7 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) message, (2) photo-message, or (3) youtube-message parameter.
CVE-2013-3526	Cross-site scripting (XSS) vulnerability in js/ta_loaded.js.php in the Traffic Analyzer plugin, possibly 3.3.2 and earlier, for WordPress allows remote attackers to inject arbitrary web script or HTML via the aid parameter.
CVE-2013-3254	Cross-site scripting (XSS) vulnerability in wp-admin/admin.php in the WP Photo Album Plus plugin before 5.0.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via the commentid parameter in a wppa_manage_comments edit action.
CVE-2013-2707	Cross-site request forgery (CSRF) vulnerability in the Login With Ajax plugin before 3.1 for WordPress allows remote attackers to hijack the authentication of arbitrary users for requests that modify this plugin's settings.
CVE-2013-2703	Cross-site request forgery (CSRF) vulnerability in the Facebook Members plugin before 5.0.5 for WordPress allows remote attackers to hijack the authentication of administrators for requests that modify this plugin's settings.
CVE-2013-2702	Cross-site request forgery (CSRF) vulnerability in the Easy AdSense Lite plugin before 6.10 for WordPress allows remote attackers to hijack the authentication of arbitrary users for requests that modify this plugin's settings.
CVE-2013-2709	Cross-site request forgery (CSRF) vulnerability in the FourSquare Checkins plugin before 1.3 for WordPress allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences.
CVE-2013-1949	Social Media Widget (social-media-widget) plugin 4.0 for WordPress contains an externally introduced modification (Trojan Horse), which allows remote attackers to force the upload of arbitrary files.

CVE-2013-2696	Cross-site request forgery (CSRF) vulnerability in the All in One Webmaster plugin before 8.2.4 for WordPress allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences.
CVE-2013-2697	Cross-site request forgery (CSRF) vulnerability in the WP-DownloadManager plugin before 1.61 for WordPress allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences.
CVE-2013-2744	importbuddy.php in the BackupBuddy plugin 2.2.25 for WordPress allows remote attackers to obtain configuration information via a step 0 phpinfo action, which calls the phpinfo function.
CVE-2013-2743	importbuddy.php in the BackupBuddy plugin 1.3.4, 2.1.4, 2.2.25, 2.2.28, and 2.2.4 for WordPress allows remote attackers to bypass authentication via a crafted integer in the step parameter.
CVE-2013-2742	importbuddy.php in the BackupBuddy plugin 1.3.4, 2.1.4, 2.2.25, 2.2.28, and 2.2.4 for WordPress does not reliably delete itself after completing a restore operation, which makes it easier for remote attackers to obtain access via subsequent requests to this script.
CVE-2013-2741	importbuddy.php in the BackupBuddy plugin 1.3.4, 2.1.4, 2.2.25, 2.2.28, and 2.2.4 for WordPress does not require that authentication be enabled, which allows remote attackers to obtain sensitive information, or overwrite or delete files, via vectors involving a (1) direct request, (2) step=1 request, (3) step=2 or step=3 request, or (4) step=7 request.
CVE-2013-2501	Cross-site scripting (XSS) vulnerability in the Terillion Reviews plugin before 1.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the ProfileId field.
CVE-2013-2640	ajax.functions.php in the MailUp plugin before 1.3.2 for WordPress does not properly restrict access to unspecified Ajax functions, which allows remote attackers to modify plugin settings and conduct cross-site scripting (XSS) attacks via unspecified vectors related to "formData=save" requests, a different version than CVE-2013-0731.
CVE-2013-0731	ajax.functions.php in the MailUp plugin before 1.3.3 for WordPress does not properly restrict access to unspecified Ajax functions, which allows remote attackers to modify plugin settings and conduct cross-site scripting (XSS) attacks by setting the wordpress_logged_in cookie. NOTE: this is due to an incomplete fix for a similar issue that was fixed in 1.3.2.
CVE-2011-5265	Cross-site scripting (XSS) vulnerability in cached_image.php in the Featurific For WordPress plugin 1.6.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the snum parameter. NOTE: this has been disputed by a third party.
CVE-2011-5264	Cross-site scripting (XSS) vulnerability in lazyest-backup.php in the Lazyest Backup plugin before 0.2.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the xml_or_all parameter.
CVE-2011-5257	Multiple cross-site scripting (XSS) vulnerabilities in the Classipress theme before 3.1.5 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) twitter_id parameter related to the Twitter widget and (2) facebook_id parameter related to the Facebook widget.
CVE-2013-1464	Cross-site scripting (XSS) vulnerability in assets/player.swf in the Audio Player plugin before 2.0.4.6 for Wordpress allows remote attackers to inject arbitrary web script or HTML via the playerID parameter.
CVE-2013-1463	Cross-site scripting (XSS) vulnerability in js/tabletools/zeroclipboard.swf in the WP-Table Reloaded module before 1.9.4 for Wordpress allows remote attackers to inject arbitrary web script or HTML via the id parameter. NOTE: this might be the same vulnerability as CVE-2013-1808. If so, it is likely that CVE-2013-1463 will be REJECTed.
CVE-2012-6527	Cross-site scripting (XSS) vulnerability in the My Calendar plugin before 1.10.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.
CVE-2012-6506	Multiple cross-site scripting (XSS) vulnerabilities in the Zingiri Web Shop plugin 2.4.0 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) page parameter in zing.inc.php or (2) notes parameter in fws/pages-front/onecheckout.php.
CVE-2011-4618	Cross-site scripting (XSS) vulnerability in advancedtext.php in Advanced Text Widget plugin before 2.0.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.
CVE-2012-6499	Open redirect vulnerability in age-verification.php in the Age Verification plugin 0.4 and earlier for WordPress allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the redirect_to parameter.
CVE-2011-5254	Unspecified vulnerability in the Connections plugin before 0.7.1.6 for WordPress has unknown impact and attack vectors.
CVE-2013-0721	wp-php-widget.php in the WP PHP widget plugin 1.0.2 for WordPress allows remote attackers to obtain sensitive information via a direct request, which reveals the full path in an error message.
CVE-2012-5868	WordPress 3.4.2 does not invalidate a wordpress_sec session cookie upon an administrator's logout action, which makes it easier for remote attackers to discover valid session identifiers via a brute-force attack, or modify data via a replay attack.
CVE-2012-5469	The Portable phpMyAdmin plugin before 1.3.1 for WordPress allows remote attackers to bypass authentication and obtain phpMyAdmin console access via a direct request to wp-content/plugins/portable-phpmyadmin/wp-pma-mod.
CVE-2012-5178	Cross-site request forgery (CSRF) vulnerability in the Welcart plugin before 1.2.2 for WordPress allows remote attackers to hijack the authentication of arbitrary users for requests that complete a purchase.
CVE-2012-5177	Cross-site scripting (XSS) vulnerability in the Welcart plugin before 1.2.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2012-6313	simple-gmail-login.php in the Simple Gmail Login plugin before 1.1.4 for WordPress allows remote attackers to obtain sensitive information via a request that lacks a timezone, leading to disclosure of the installation path in a stack trace.
CVE-2012-6312	Cross-site scripting (XSS) vulnerability in the Video Lead Form plugin for WordPress allows remote attackers to inject arbitrary web script or HTML via the errMsg parameter in a video-lead-form action to wp-admin/admin.php.
CVE-2012-5913	Cross-site scripting (XSS) vulnerability in wp-integrator.php in the WordPress Integrator module 1.32 for WordPress allows remote attackers to inject arbitrary web script or HTML via the redirect_to parameter to wp-login.php.
CVE-2012-5856	Cross-site scripting (XSS) vulnerability in the Uk Cookie (aka uk-cookie) plugin for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-5226	Cross-site request forgery (CSRF) vulnerability in wordpress_sentinel.php in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to hijack the authentication of an administrator for requests that trigger snapshots.
CVE-2011-5225	Cross-site scripting (XSS) vulnerability in wordpress_sentinel.php in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via unknown vectors.
CVE-2011-5224	SQL injection vulnerability in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors.
CVE-2011-5216	SQL injection vulnerability in ajax.php in SCORM Cloud For WordPress plugin before 1.0.7 for WordPress allows remote attackers to execute arbitrary SQL commands via the active parameter. NOTE: some of these details are obtained from third party information.
CVE-2012-5388	Cross-site scripting (XSS) vulnerability in wlcms-plugin.php in the White Label CMS plugin 1.5 for WordPress allows remote authenticated administrators to inject arbitrary web script or HTML via the wlcms_o_developer_name parameter in a save action to wp-admin/admin.php, a related issue to CVE-2012-5387.
CVE-2012-5387	Cross-site request forgery (CSRF) vulnerability in wlcms-plugin.php in the White Label CMS plugin before 1.5.1 for WordPress allows remote attackers to hijack the authentication of administrators for requests that modify the developer name via the wlcms_o_developer_name parameter in a save action to wp-admin/admin.php, as demonstrated by a developer name containing XSS sequences.
CVE-2012-5350	SQL injection vulnerability in the Pay With Tweet plugin before 1.2 for WordPress allows remote authenticated users with certain permissions to execute arbitrary SQL commands via the id parameter in a paywithtweet shortcode.
CVE-2012-5349	Multiple cross-site scripting (XSS) vulnerabilities in pay.php in the Pay With Tweet plugin before 1.2 allow remote attackers to inject arbitrary web script or HTML via the (1) link, (2) title, or (3) dl parameter.
CVE-2012-5346	Cross-site scripting (XSS) vulnerability in wp-live.php in the WP Live.php module 1.2.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter. NOTE: some of these details are obtained from third party information.
CVE-2012-5328	Multiple SQL injection vulnerabilities in the Mingle Forum plugin 1.0.32.1 and other versions before 1.0.33 for WordPress might allow remote authenticated users to execute arbitrary SQL commands via the (1) memberid or (2) groupid parameters in a removemember action or (3) id parameter to fs-admin/fs-admin.php, or (4) edit_forum_id parameter in an edit_save_forum action to fs-admin/wpf-edit-forum-group.php.
CVE-2012-5327	Multiple SQL injection vulnerabilities in fs-admin/fs-admin.php in the Mingle Forum plugin 1.0.32.1 and other versions before 1.0.33 for WordPress allow remote authenticated users to execute arbitrary SQL commands via the (1) delete_usrgrp[] parameter in a delete_usergroups action, (2) usergroup parameter in an add_user_togroup action, or (3) add_forum_group_id parameter in an add_forum_submit action.
CVE-2012-5325	Multiple cross-site scripting (XSS) vulnerabilities in the scr_do_redirect function in scr.php in the Shortcode Redirect plugin 1.0.01 and earlier for WordPress allow remote authenticated users with certain permissions to inject arbitrary web script or HTML via the (1) url or (2) sec attributes in a redirect tag.
CVE-2011-5208	Multiple directory traversal vulnerabilities in the BackWPup plugin before 1.4.1 for WordPress allow remote attackers to read arbitrary files via a .. (dot dot) in the wpabs parameter to (1) app/options-view_log-iframe.php or (2) app/options-runnow-iframe.php.
CVE-2011-4342	PHP remote file inclusion vulnerability in wp_xml_export.php in the BackWPup plugin before 1.7.2 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the wpabs parameter.
CVE-2012-5318	Unrestricted file upload vulnerability in uploadify/scripts/uploadify.php in the Kish Guest Posting plugin 1.2 for WordPress allows remote attackers to execute arbitrary code by uploading a file with a double extension, then accessing it via a direct request to the file in the directory specified by the folder parameter. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1125.
CVE-2012-5310	SQL injection vulnerability in the WP e-Commerce plugin before 3.8.7.6 for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors.
CVE-2012-1125	Unrestricted file upload vulnerability in uploadify/scripts/uploadify.php in the Kish Guest Posting plugin before 1.2 for WordPress allows remote attackers to execute arbitrary code by uploading a file with a PHP extension, then accessing it via a direct request to the file in the directory specified by the folder parameter.

CVE-2011-5207	Cross-site scripting (XSS) vulnerability in admin/OptionsPostsList.php in the TheCartPress plugin for WordPress before 1.1.6 before 2011-12-31 allows remote attackers to inject arbitrary web script or HTML via the <code>tcp_name_post_XXXXX</code> parameter.
CVE-2012-4242	Cross-site scripting (XSS) vulnerability in the MF Gig Calendar plugin 0.9.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the query string to the calendar page.
CVE-2012-5229	Cross-site scripting (XSS) vulnerability in css/gallery-css.php in the Slideshow Gallery2 plugin for WordPress allows remote attackers to inject arbitrary web script or HTML via the border parameter.
CVE-2012-4448	Cross-site request forgery (CSRF) vulnerability in wp-admin/index.php in WordPress 3.4.2 allows remote attackers to hijack the authentication of administrators for requests that modify an RSS URL via a <code>dashboard_incoming_links</code> edit action.
CVE-2011-5194	Cross-site scripting (XSS) vulnerability in vendors/samswhois/samswhois.inc.php in the Whois Search plugin before 1.4.2.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via the domain parameter, a different vulnerability than CVE-2011-5193.
CVE-2011-5193	Cross-site scripting (XSS) vulnerability in vendors/samswhois/samswhois.inc.php in the Whois Search plugin 1.4.2.3 for WordPress, when the WHOIS widget is enabled, allows remote attackers to inject arbitrary web script or HTML via the domain parameter to index.php, a different vulnerability than CVE-2011-5194.
CVE-2011-5192	Cross-site scripting (XSS) vulnerability in pretty-bar.php in Pretty Link Lite plugin before 1.5.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the slug parameter, a different vulnerability than CVE-2011-5191.
CVE-2011-5191	Cross-site scripting (XSS) vulnerability in pretty-bar.php in Pretty Link Lite plugin before 1.5.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the slug parameter, a different vulnerability than CVE-2011-5192.
CVE-2011-5182	** DISPUTED ** Cross-site scripting (XSS) vulnerability in lanoba-social-plugin/index.php in the Lanoba Social plugin 1.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via the action parameter. NOTE: the vendor disputes this issue, stating "Lanoba's plug in does sanitize user input, and because that input is never sent to the browser, an attacker has no way of executing script or code on a user's behalf."
CVE-2011-5181	Cross-site scripting (XSS) vulnerability in clickdesk.php in ClickDesk Live Support - Live Chat plugin 2.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cdwidgetid parameter. NOTE: some of these details are obtained from third party information.
CVE-2011-5180	Cross-site scripting (XSS) vulnerability in wp-1pluginjquery.php in the ZooEffect plugin 1.01 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter. NOTE: some of these details are obtained from third party information. NOTE: this has been disputed by a third party.
CVE-2011-5179	Cross-site scripting (XSS) vulnerability in skysa-official/skysa.php in Skysa App Bar Integration plugin, possibly before 1.04, for WordPress allows remote attackers to inject arbitrary web script or HTML via the submit parameter.
CVE-2012-4422	wp-admin/plugins.php in WordPress before 3.4.2, when the multisite feature is enabled, does not check for network-administrator privileges before performing a network-wide activation of an installed plugin, which might allow remote authenticated users to make unintended plugin changes by leveraging the Administrator role.
CVE-2012-4421	The <code>create_post</code> function in wp-includes/class-wp-atom-server.php in WordPress before 3.4.2 does not perform a capability check, which allows remote authenticated users to bypass intended access restrictions and publish new posts by leveraging the Contributor role and using the Atom Publishing Protocol (aka AtomPub) feature.
CVE-2010-5106	The XML-RPC remote publishing interface in xmlrpc.php in WordPress before 3.0.3 does not properly check capabilities, which allows remote authenticated users to bypass intended access restrictions, and publish, edit, or delete posts, by leveraging the Author or Contributor role.
CVE-2012-4874	Unspecified vulnerability in the Another WordPress Classifieds Plugin before 2.0 for WordPress has unknown impact and attack vectors related to "image uploads."
CVE-2012-2109	SQL injection vulnerability in wp-load.php in the BuddyPress plugin 1.5.x before 1.5.5 of WordPress allows remote attackers to execute arbitrary SQL commands via the page parameter in an <code>activity_widget_filter</code> action.
CVE-2011-5128	Multiple cross-site scripting (XSS) vulnerabilities in the Adminimize plugin before 1.7.22 for WordPress allow remote attackers to inject arbitrary web script or HTML via the page parameter to (1) inc-options/deinstall_options.php, (2) inc-options/theme_options.php, or (3) inc-options/im_export_options.php, or the (4) post or (5) post_ID parameters to adminimize.php, different vectors than CVE-2011-4926.
CVE-2011-4926	Cross-site scripting (XSS) vulnerability in adminimize/adminimize_page.php in the Adminimize plugin before 1.7.22 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.
CVE-2011-5107	Cross-site scripting (XSS) vulnerability in post_alert.php in Alert Before Your Post plugin, possibly 0.1.1 and earlier, for WordPress allows remote attackers to inject arbitrary web script or HTML via the name parameter.
CVE-2011-5106	Cross-site scripting (XSS) vulnerability in edit-post.php in the Flexible Custom Post Type plugin before 0.1.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the id parameter.
CVE-2011-5104	Cross-site scripting (XSS) vulnerability in wpse-admin/display-sales-logs.php in WP e-Commerce plugin 3.8.7.1 and possibly earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the custom_text parameter. NOTE: some of these details are obtained from third party information.

CVE-2012-3434	Multiple cross-site scripting (XSS) vulnerabilities in userperspan.php in the Count Per Day module before 3.2 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) page, (2) datemin, or (3) datemax parameter.
CVE-2012-4332	The ShareYourCart plugin 1.7.1 for WordPress allows remote attackers to obtain the installation path via unspecified vectors related to the SDK.
CVE-2012-4327	Unspecified vulnerability in the Image News slider plugin before 3.3 for WordPress has unspecified impact and remote attack vectors.
CVE-2012-1835	Multiple cross-site scripting (XSS) vulnerabilities in the All-in-One Event Calendar plugin 1.4 and 1.5 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) title parameter to app/view/agenda-widget-form.php; (2) args, (3) title, (4) before_title, or (5) after_title parameter to app/view/agenda-widget.php; (6) button_value parameter to app/view/box_publish_button.php; or (7) msg parameter to /app/view/save_successful.php.
CVE-2012-4283	Cross-site scripting (XSS) vulnerability in the Login With Ajax plugin before 3.0.4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the callback parameter.
CVE-2012-4273	Cross-site scripting (XSS) vulnerability in libs/xing.php in the 2 Click Social Media Buttons plugin before 0.34 for WordPress allows remote attackers to inject arbitrary web script or HTML via the xing-url parameter.
CVE-2012-4272	Multiple cross-site scripting (XSS) vulnerabilities in the 2 Click Social Media Buttons plugin before 0.34 for WordPress allow remote attackers to inject arbitrary web script or HTML via unspecified vectors related to the "processing of the buttons of Xing and Pinterest".
CVE-2012-4271	Multiple cross-site scripting (XSS) vulnerabilities in bad-behavior-wordpress-admin.php in the Bad Behavior plugin before 2.0.47 and 2.2.x before 2.2.5 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) PATH_INFO, (2) httpbl_key, (3) httpbl_maxage, (4) httpbl_threat, (5) reverse_proxy_addresses, or (6) reverse_proxy_header parameter.
CVE-2012-4268	Cross-site scripting (XSS) vulnerability in bulletproof-security/admin/options.php in the BulletProof Security plugin before .47.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the HTTP_ACCEPT_ENCODING header.
CVE-2012-4264	Multiple cross-site scripting (XSS) vulnerabilities in the Better WP Security (better_wp_security) plugin before 3.2.5 for WordPress allow remote attackers to inject arbitrary web script or HTML via unspecified vectors related to "server variables," a different vulnerability than CVE-2012-4263.
CVE-2012-4263	Cross-site scripting (XSS) vulnerability in inc/admin/content.php in the Better WP Security (better_wp_security) plugin before 3.2.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the HTTP_USER_AGENT header.
CVE-2012-2371	Cross-site scripting (XSS) vulnerability in index.php in the WP-FaceThumb plugin 0.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the pagination_wp_facethumb parameter.
CVE-2012-3385	WordPress before 3.4.1 does not properly restrict access to post contents such as private or draft posts, which allows remote authors or contributors to obtain sensitive information via unknown vectors.
CVE-2012-3384	Cross-site request forgery (CSRF) vulnerability in the customizer in WordPress before 3.4.1 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.
CVE-2012-3383	The map_meta_cap function in wp-includes/capabilities.php in WordPress 3.4.x before 3.4.2, when the multisite feature is enabled, does not properly assign the unfiltered_html capability, which allows remote authenticated users to bypass intended access restrictions and conduct cross-site scripting (XSS) attacks by leveraging the Administrator or Editor role and composing crafted text.
CVE-2012-4033	Multiple unspecified vulnerabilities in the Zingiri Web Shop plugin before 2.4.0 for WordPress have unknown impact and attack vectors.
CVE-2012-3814	Unrestricted file upload vulnerability in font-upload.php in the Font Uploader plugin 1.2.4 for WordPress allows remote attackers to execute arbitrary PHP code by uploading a PHP file with a .php.ttf extension, then accessing it via a direct request to the file in font-uploader/fonts.
CVE-2011-4957	The make_clickable function in wp-includes/formatting.php in WordPress before 3.1.1 does not properly check URLs before passing them to the PCRE library, which allows remote attackers to cause a denial of service (crash) via a comment with a crafted URL that triggers many recursive calls.
CVE-2011-4956	Cross-site scripting (XSS) vulnerability in WordPress before 3.1.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-3588	Directory traversal vulnerability in preview.php in the Plugin Newsletter plugin 1.5 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the data parameter.
CVE-2012-3578	Unrestricted file upload vulnerability in html/Upload.php in the FCChat Widget plugin 2.2.13.1 and earlier for WordPress allows remote attackers to execute arbitrary code by uploading a file with a file with an executable extension followed by a safe extension, then accessing it via a direct request to the file in html/images.
CVE-2012-3577	Unrestricted file upload vulnerability in douload.php in the Nmedia Member Conversation plugin before 1.4 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in wp-content/uploads/user_uploads.

CVE-2012-3576	Unrestricted file upload vulnerability in php/upload.php in the wpStoreCart plugin before 2.5.30 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in uploads/wpstorecart.
CVE-2012-3575	Unrestricted file upload vulnerability in uploader.php in the RBX Gallery plugin 2.1 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in uploads/rbxslider.
CVE-2012-3574	Unrestricted file upload vulnerability in includes/doajaxfileupload.php in the MM Forms Community plugin 2.2.5 and 2.2.6 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in upload/temp.
CVE-2012-2759	Cross-site scripting (XSS) vulnerability in login-with-ajax.php in the Login With Ajax (aka login-with-ajax) plugin before 3.0.4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the callback parameter in a lostpassword action to wp-login.php.
CVE-2012-2920	Cross-site scripting (XSS) vulnerability in the userphoto_options_page function in user-photo.php in the User Photo plugin before 0.9.5.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to wp-admin/options-general.php. NOTE: some of these details are obtained from third party information.
CVE-2012-2917	Cross-site scripting (XSS) vulnerability in the Share and Follow plugin 1.80.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via the CDN API Key (cdn-key) in a share-and-follow-menu page to wp-admin/admin.php.
CVE-2012-2916	Cross-site scripting (XSS) vulnerability in sabre_class_admin.php in the SABRE plugin before 2.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the active_option parameter to wp-admin/tools.php.
CVE-2012-2913	Multiple cross-site scripting (XSS) vulnerabilities in the Leaflet plugin 0.0.1 for WordPress allow remote attackers to inject arbitrary web script or HTML via the id parameter to (1) leaflet_layer.php or (2) leaflet_marker.php, as reachable through wp-admin/admin.php.
CVE-2012-2912	Multiple cross-site scripting (XSS) vulnerabilities in the LeagueManager plugin 3.7 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) group parameter in the show-league page or (2) season parameter in the team page to wp-admin/admin.php.
CVE-2012-1936	** DISPUTED ** The wp_create_nonce function in wp-includes/pluggable.php in WordPress 3.3.1 and earlier associates a nonce with a user account instead of a user session, which might make it easier for remote attackers to conduct cross-site request forgery (CSRF) attacks on specific actions and objects by sniffing the network, as demonstrated by attacks against the wp-admin/admin-ajax.php and wp-admin/user-new.php scripts. NOTE: the vendor reportedly disputes the significance of this issue because wp_create_nonce operates as intended, even if it is arguably inconsistent with certain CSRF protection details advocated by external organizations.
CVE-2012-2404	wp-comments-post.php in WordPress before 3.3.2 supports offsite redirects, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.
CVE-2012-2403	wp-includes/formatting.php in WordPress before 3.3.2 attempts to enable clickable links inside attributes, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.
CVE-2012-2402	wp-admin/plugins.php in WordPress before 3.3.2 allows remote authenticated site administrators to bypass intended access restrictions and deactivate network-wide plugins via unspecified vectors.
CVE-2012-2401	Plupload before 1.5.4, as used in wp-includes/js/plupload/ in WordPress before 3.3.2 and other products, enables scripting regardless of the domain from which the SWF content was loaded, which allows remote attackers to bypass the Same Origin Policy via crafted content.
CVE-2012-2400	Unspecified vulnerability in wp-includes/js/swfobject.js in WordPress before 3.3.2 has unknown impact and attack vectors.
CVE-2012-2399	Cross-site scripting (XSS) vulnerability in swfupload.swf in SWFupload 2.2.0.1 and earlier, as used in WordPress before 3.5.2, TinyMCE Image Manager 1.1 and earlier, and other products allows remote attackers to inject arbitrary web script or HTML via the buttonText parameter, a different vulnerability than CVE-2012-3414.
CVE-2012-1786	The Media Upload form in the Video Embed & Thumbnail Generator plugin before 2.0 for WordPress allows remote attackers to obtain the installation path via unknown vectors.
CVE-2012-1785	kg_callffmpeg.php in the Video Embed & Thumbnail Generator plugin before 2.0 for WordPress allows remote attackers to execute arbitrary commands via unspecified vectors.
CVE-2011-5082	Cross-site scripting (XSS) vulnerability in the s2Member Pro plugin before 111220 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s2member_pro_authnet_checkout[coupon] parameter (aka Coupon Code field).
CVE-2012-1205	PHP remote file inclusion vulnerability in relocate-upload.php in Relocate Upload plugin before 0.20 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.
CVE-2012-1068	Cross-site scripting (XSS) vulnerability in the rc_ajax function in core.php in the WP-RecentComments plugin before 2.0.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter, related to AJAX paging.

CVE-2012-1067	SQL injection vulnerability in the WP-RecentComments plugin 2.0.7 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter in an rc-content action to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2012-1011	actions.php in the AllWebMenus plugin 1.1.8 for WordPress allows remote attackers to bypass intended access restrictions to upload and execute arbitrary PHP code by setting the HTTP_REFERER to a certain value, then uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.
CVE-2012-1010	Unrestricted file upload vulnerability in actions.php in the AllWebMenus plugin before 1.1.8 for WordPress allows remote attackers to execute arbitrary PHP code by uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.
CVE-2012-0937	** DISPUTED ** wp-admin/setup-config.php in the installation component in WordPress 3.3.1 and earlier does not limit the number of MySQL queries sent to external MySQL database servers, which allows remote attackers to use WordPress as a proxy for brute-force attacks or denial of service attacks via the dbhost parameter, a different vulnerability than CVE-2011-4898. NOTE: the vendor disputes the significance of this issue because an incomplete WordPress installation might be present on the network for only a short time.
CVE-2012-0782	** DISPUTED ** Multiple cross-site scripting (XSS) vulnerabilities in wp-admin/setup-config.php in the installation component in WordPress 3.3.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) dbhost, (2) dbname, or (3) uname parameter. NOTE: the vendor disputes the significance of this issue; also, it is unclear whether this specific XSS scenario has security relevance.
CVE-2011-4899	** DISPUTED ** wp-admin/setup-config.php in the installation component in WordPress 3.3.1 and earlier does not ensure that the specified MySQL database service is appropriate, which allows remote attackers to configure an arbitrary database via the dbhost and dbname parameters, and subsequently conduct static code injection and cross-site scripting (XSS) attacks via (1) an HTTP request or (2) a MySQL query. NOTE: the vendor disputes the significance of this issue; however, remote code execution makes the issue important in many realistic environments.
CVE-2011-4898	** DISPUTED ** wp-admin/setup-config.php in the installation component in WordPress 3.3.1 and earlier generates different error messages for requests lacking a dbname parameter depending on whether the MySQL credentials are valid, which makes it easier for remote attackers to conduct brute-force attacks via a series of requests with different uname and pwd parameters. NOTE: the vendor disputes the significance of this issue; also, it is unclear whether providing intentionally vague error messages during installation would be reasonable from a usability perspective.
CVE-2012-0934	PHP remote file inclusion vulnerability in ajax/savetag.php in the Theme Tuner plugin for WordPress before 0.8 allows remote attackers to execute arbitrary PHP code via a URL in the tt-abspath parameter.
CVE-2012-0898	Directory traversal vulnerability in meb_download.php in the myEASYbackup plugin 1.0.8.1 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the dwn_file parameter.
CVE-2012-0896	Absolute path traversal vulnerability in download.php in the Count Per Day module before 3.1.1 for WordPress allows remote attackers to read arbitrary files via the f parameter.
CVE-2012-0895	Cross-site scripting (XSS) vulnerability in map/map.php in the Count Per Day module before 3.1.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the map parameter.
CVE-2012-0287	Cross-site scripting (XSS) vulnerability in wp-comments-post.php in WordPress 3.3.x before 3.3.1, when Internet Explorer is used, allows remote attackers to inject arbitrary web script or HTML via the query string in a POST operation that is not properly handled by the "Duplicate comment detected" feature.
CVE-2011-5051	Multiple unrestricted file upload vulnerabilities in the WP Symposium plugin before 11.12.24 for WordPress allow remote attackers to execute arbitrary code by uploading a file with an executable extension using (1) uploadify/upload_admin_avatar.php or (2) uploadify/upload_profile_avatar.php, then accessing it via a direct request to the file in an unspecified directory inside the webroot.
CVE-2011-3841	Cross-site scripting (XSS) vulnerability in uploadify/get_profile_avatar.php in the WP Symposium plugin before 11.12.08 for WordPress allows remote attackers to inject arbitrary web script or HTML via the uid parameter.
CVE-2011-4803	SQL injection vulnerability in wptouch/ajax.php in the WPTouch plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
CVE-2011-4673	SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
CVE-2011-4671	SQL injection vulnerability in adrotate/adrotate-out.php in the AdRotate plugin 3.6.6, and other versions before 3.6.8, for WordPress allows remote attackers to execute arbitrary SQL commands via the track parameter (aka redirect URL).
CVE-2011-4669	SQL injection vulnerability in wp-users.php in WordPress Users plugin 1.3 and possibly earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the uid parameter to index.php.
CVE-2011-4646	SQL injection vulnerability in wp-postratings.php in the WP-Post Ratings plugin 1.50, 1.61, and probably other versions before 1.62 for WordPress allows remote authenticated users with the Author role to execute arbitrary SQL commands via the id attribute of the ratings shortcode when creating a post. NOTE: some of these details are obtained from third party information.

CVE-2011-4568	Cross-site scripting (XSS) vulnerability in view/frontend-head.php in the Flowplayer plugin before 1.2.12 for WordPress allows remote attackers to inject arbitrary web script or HTML via the URI.
CVE-2011-4562	Multiple cross-site scripting (XSS) vulnerabilities in (1) view/admin/log_item.php and (2) view/admin/log_item_details.php in the Redirection plugin 2.2.9 for WordPress allow remote attackers to inject arbitrary web script or HTML via the Referer HTTP header in a request to a post that does not exist.
CVE-2010-4875	Cross-site scripting (XSS) vulnerability in vodpod-video-gallery/vodpod_gallery_thumbs.php in the Vodpod Video Gallery Plugin 3.1.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the gid parameter.
CVE-2011-3981	PHP remote file inclusion vulnerability in actions.php in the Allwebmenus plugin 1.1.3 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.
CVE-2011-3865	Cross-site scripting (XSS) vulnerability in the Black-LetterHead theme before 1.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to index.php.
CVE-2011-3864	Cross-site scripting (XSS) vulnerability in the The Erudite theme before 2.7.9 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cpage parameter.
CVE-2011-3863	Cross-site scripting (XSS) vulnerability in the RedLine theme before 1.66 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3862	Cross-site scripting (XSS) vulnerability in the Morning Coffee theme before 3.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to index.php.
CVE-2011-3861	Cross-site scripting (XSS) vulnerability in the Web Minimalist 200901 theme before 1.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to index.php.
CVE-2011-3860	Cross-site scripting (XSS) vulnerability in the Cover WP theme before 1.6.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3859	Cross-site scripting (XSS) vulnerability in the Trending theme before 0.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cpage parameter.
CVE-2011-3858	Cross-site scripting (XSS) vulnerability in the Pixiv Custom theme before 2.1.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3857	Cross-site scripting (XSS) vulnerability in the Antisnews theme before 1.10 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3856	Cross-site scripting (XSS) vulnerability in the Elegant Grunge theme before 1.0.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3855	Cross-site scripting (XSS) vulnerability in the F8 Lite theme before 4.2.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3854	Cross-site scripting (XSS) vulnerability in the ZenLite theme before 4.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3853	Cross-site scripting (XSS) vulnerability in the Hybrid theme before 0.10 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cpage parameter.
CVE-2011-3852	Cross-site scripting (XSS) vulnerability in the EvoLve theme before 1.2.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3851	Cross-site scripting (XSS) vulnerability in the News theme before 0.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cpage parameter.
CVE-2011-3850	Cross-site scripting (XSS) vulnerability in the Atahualpa theme before 3.6.8 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.
CVE-2011-3818	WordPress 2.9.2 and 3.0.4 allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message, as demonstrated by wp-admin/includes/user.php and certain other files.
CVE-2010-4839	SQL injection vulnerability in the Event Registration plugin 5.32 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the event_id parameter in a register action.
CVE-2010-4825	Cross-site scripting (XSS) vulnerability in magpie_debug.php in the Twitter Feed plugin (wp-twitter-feed) 0.3.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the url parameter.
CVE-2011-3130	wp-includes/taxonomy.php in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 has unknown impact and attack vectors related to "Taxonomy query hardening," possibly involving SQL injection.
CVE-2011-3129	The file upload functionality in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2, when running "on hosts with dangerous security settings," has unknown impact and attack vectors, possibly related to dangerous filenames.
CVE-2011-3128	WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 treats unattached attachments as published, which might allow remote attackers to obtain sensitive data via vectors related to wp-includes/post.php.
CVE-2011-3127	WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 does not prevent rendering for (1) admin or (2) login pages inside a frame in a third-party HTML document, which makes it easier for remote attackers to conduct clickjacking attacks via a crafted web site.
CVE-2011-3126	WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 allows remote attackers to determine usernames of non-authors via canonical redirects.

CVE-2011-3125	Unspecified vulnerability in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 has unknown impact and attack vectors related to "Various security hardening."
CVE-2011-3122	Unspecified vulnerability in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 has unknown impact and attack vectors related to "Media security."
CVE-2011-1669	Directory traversal vulnerability in wp-download.php in the WP Custom Pages module 0.5.0.1 for WordPress allows remote attackers to read arbitrary files via ..%2F (encoded dot dot) sequences in the url parameter.
CVE-2010-4779	Cross-site scripting (XSS) vulnerability in lib/includes/auth.inc.php in the WPtouch plugin 1.9.19.4 and 1.9.20 for WordPress allows remote attackers to inject arbitrary web script or HTML via the wptouch_settings parameter to include/adsense-new.php. NOTE: some of these details are obtained from third party information.
CVE-2011-0760	Multiple cross-site request forgery (CSRF) vulnerabilities in the configuration screen in wp-relatedposts.php in the WP Related Posts plugin 1.0 for WordPress allow remote attackers to hijack the authentication of administrators for requests that insert cross-site scripting (XSS) sequences via the (1) wp_relatedposts_title, (2) wp_relatedposts_num, or (3) wp_relatedposts_type parameter.
CVE-2011-0759	Multiple cross-site request forgery (CSRF) vulnerabilities in the configuration page in the Recaptcha (aka WP-reCAPTCHA) plugin 2.9.8.2 for WordPress allow remote attackers to hijack the authentication of administrators for requests that disable the CAPTCHA requirement or insert cross-site scripting (XSS) sequences via the (1) recaptcha_opt_pubkey, (2) recaptcha_opt_privkey, (3) re_tabindex, (4) error_blank, (5) error_incorrect, (6) mailhide_pub, (7) mailhide_priv, (8) mh_replace_link, or (9) mh_replace_title parameter.
CVE-2011-0701	wp-admin/async-upload.php in the media uploader in WordPress before 3.0.5 allows remote authenticated users to read (1) draft posts or (2) private posts via a modified attachment_id parameter.
CVE-2011-0700	Multiple cross-site scripting (XSS) vulnerabilities in WordPress before 3.0.5 allow remote authenticated users to inject arbitrary web script or HTML via vectors related to (1) the Quick/Bulk Edit title (aka post title or post_title), (2) post_status, (3) comment_status, (4) ping_status, and (5) escaping of tags within the tags meta box.
CVE-2010-4747	Cross-site scripting (XSS) vulnerability in wordpress-processing-embed/data/popup.php in the Processing Embed plugin 0.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the pluginurl parameter.
CVE-2011-1047	Multiple SQL injection vulnerabilities in VastHTML Forum Server (aka ForumPress) plugin 1.6.1 and 1.6.5 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) search_max parameter in a search action to index.php, which is not properly handled by wpf.class.php, (2) id parameter in an editpost action to index.php, which is not properly handled by wpf-post.php, or (3) topic parameter to feed.php.
CVE-2011-0740	Cross-site scripting (XSS) vulnerability in magpie/scripts/magpie_slashbox.php in RSS Feed Reader 0.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the rss_url parameter.
CVE-2011-0641	Multiple cross-site scripting (XSS) vulnerabilities in wp-admin/admin.php in the StatPressCN plugin 1.9.0 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) what1, (2) what2, (3) what3, (4) what4, and (5) what5 parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2010-4536	Multiple cross-site scripting (XSS) vulnerabilities in KSES, as used in WordPress before 3.0.4, allow remote attackers to inject arbitrary web script or HTML via vectors related to (1) the & (ampersand) character, (2) the case of an attribute name, (3) a padded entity, and (4) an entity that is not in normalized form.
CVE-2010-4637	Cross-site scripting (XSS) vulnerability in feedlist/handler_image.php in the FeedList plugin 2.61.01 for WordPress allows remote attackers to inject arbitrary web script or HTML via the i parameter.
CVE-2010-4630	Cross-site scripting (XSS) vulnerability in pages/admin/surveys/create.php in the WP Survey And Quiz Tool plugin 1.2.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the action parameter.
CVE-2010-4277	Cross-site scripting (XSS) vulnerability in lembbedded-video.php in the Embedded Video plugin 4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the content parameter to wp-admin/post.php.
CVE-2010-4518	Cross-site scripting (XSS) vulnerability in wp-safe-search/wp-safe-search-jx.php in the Safe Search plugin 0.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the v1 parameter.
CVE-2010-4257	SQL injection vulnerability in the do_trackbacks function in wp-includes/comment.php in WordPress before 3.0.2 allows remote authenticated users to execute arbitrary SQL commands via the Send Trackbacks field.
CVE-2010-4403	The Register Plus plugin 3.5.1 and earlier for WordPress allows remote attackers to obtain sensitive information via a direct request to (1) dash_widget.php and (2) register-plus.php, which reveals the installation path in an error message.
CVE-2010-4402	Multiple cross-site scripting (XSS) vulnerabilities in wp-login.php in the Register Plus plugin 3.5.1 and earlier for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) firstname, (2) lastname, (3) website, (4) aim, (5) yahoo, (6) jabber, (7) about, (8) pass1, and (9) pass2 parameters in a register action.
CVE-2010-3977	Multiple cross-site scripting (XSS) vulnerabilities in wp-content/plugins/cforms/lib_ajax.php in cforms WordPress plugin 11.5 allow remote attackers to inject arbitrary web script or HTML via the (1) rs and (2) rsargs[] parameters.
CVE-2010-2924	SQL injection vulnerability in myLDlinker.php in the myLinksDump Plugin 1.2 for WordPress allows remote attackers to execute arbitrary SQL commands via the url parameter. NOTE: some of these details are obtained from third party information.

CVE-2010-1186	Cross-site scripting (XSS) vulnerability in xml/media-rss.php in the NextGEN Gallery plugin before 1.5.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the mode parameter.
CVE-2009-4748	SQL injection vulnerability in mycategoryorder.php in the My Category Order plugin 2.8 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the parentID parameter in an act_OrderCategories action to wp-admin/post-new.php.
CVE-2009-4672	Directory traversal vulnerability in main.php in the WP-Lytebox plugin 1.3 for WordPress allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the pg parameter.
CVE-2010-0682	WordPress 2.9 before 2.9.2 allows remote authenticated users to read trash posts from other authors via a direct request with a modified p parameter.
CVE-2010-0673	SQL injection vulnerability in cplphoto.php in the Copperleaf Photolog plugin 0.16, and possibly earlier, for WordPress allows remote attackers to execute arbitrary SQL commands via the postid parameter.
CVE-2009-4424	SQL injection vulnerability in results.php in the Pyrmont plugin 2 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
CVE-2009-3703	Multiple SQL injection vulnerabilities in the WP-Forum plugin before 2.4 for WordPress allow remote attackers to execute arbitrary SQL commands via (1) the search_max parameter in a search action to the default URI, related to wpf.class.php; (2) the forum parameter to an unspecified component, related to wpf.class.php; (3) the topic parameter in a viewforum action to the default URI, related to the remove_topic function in wpf.class.php; or the id parameter in a (4) editpost or (5) viewtopic action to the default URI, related to wpf-post.php.
CVE-2009-4170	WP-Cumulus Plug-in 1.20 for WordPress, and possibly other versions, allows remote attackers to obtain sensitive information via a crafted request to wp-cumulus.php, probably without parameters, which reveals the installation path in an error message.
CVE-2009-4169	Cross-site scripting (XSS) vulnerability in wp-cumulus.php in the WP-Cumulus Plug-in before 1.22 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2009-4168	Cross-site scripting (XSS) vulnerability in Roy Tanck tagcloud.swf, as used in the WP-Cumulus plugin before 1.23 for WordPress and the Joomulus module 2.0 and earlier for Joomla!, allows remote attackers to inject arbitrary web script or HTML via the tagcloud parameter in a tags action. Cross-site scripting (XSS) vulnerability in tagcloud.swf in the WP-Cumulus Plug-in before 1.23 for WordPress allows remote attackers to inject arbitrary web script or HTML via the tagcloud parameter.
CVE-2009-3891	Cross-site scripting (XSS) vulnerability in wp-admin/press-this.php in WordPress before 2.8.6 allows remote authenticated users to inject arbitrary web script or HTML via the s parameter (aka the selection variable).
CVE-2009-3890	Unrestricted file upload vulnerability in the wp_check_filetype function in wp-includes/functions.php in WordPress before 2.8.6, when a certain configuration of the mod_mime module in the Apache HTTP Server is enabled, allows remote authenticated users to execute arbitrary code by posting an attachment with a multiple-extension filename, and then accessing this attachment via a direct request to a wp-content/uploads/ pathname, as demonstrated by a .php.jpg filename.
CVE-2009-3622	Algorithmic complexity vulnerability in wp-trackback.php in WordPress before 2.8.5 allows remote attackers to cause a denial of service (CPU consumption and server hang) via a long title parameter in conjunction with a charset parameter composed of many comma-separated "UTF-8" substrings, related to the mb_convert_encoding function in PHP.
CVE-2008-7175	Cross-site scripting (XSS) vulnerability in wp-admin/admin.php in NextGEN Gallery 0.96 and earlier plugin for Wordpress allows remote attackers to inject arbitrary web script or HTML via the picture description field in a page edit action.
CVE-2008-7040	SQL injection vulnerability in ahah/sf-profile.php in the Yellow Swordfish Simple Forum module for Wordpress allows remote attackers to execute arbitrary SQL commands via the u parameter. NOTE: this issue was disclosed by an unreliable researcher, so the details might be incorrect.
CVE-2009-2854	Wordpress before 2.8.3 does not check capabilities for certain actions, which allows remote attackers to make unauthorized edits or additions via a direct request to (1) edit-comments.php, (2) edit-pages.php, (3) edit.php, (4) edit-category-form.php, (5) edit-link-category-form.php, (6) edit-tag-form.php, (7) export.php, (8) import.php, or (9) link-add.php in wp-admin/.
CVE-2009-2853	Wordpress before 2.8.3 allows remote attackers to gain privileges via a direct request to (1) admin-footer.php, (2) edit-category-form.php, (3) edit-form-advanced.php, (4) edit-form-comment.php, (5) edit-link-category-form.php, (6) edit-link-form.php, (7) edit-page-form.php, and (8) edit-tag-form.php in wp-admin/.
CVE-2009-2852	WP-Syntax plugin 0.9.1 and earlier for Wordpress, with register_globals enabled, allows remote attackers to execute arbitrary PHP code via the test_filter[wp_head] array parameter to test/index.php, which is used in a call to the call_user_func_array function.
CVE-2009-2851	Cross-site scripting (XSS) vulnerability in the administrator interface in WordPress before 2.8.2 allows remote attackers to inject arbitrary web script or HTML via a comment author URL.
CVE-2009-2762	wp-login.php in WordPress 2.8.3 and earlier allows remote attackers to force a password reset for the first user in the database, possibly the administrator, via a key[] array variable in a resetpass (aka rp) action, which bypasses a check that assumes that \$key is not an array.

CVE-2009-2432	WordPress and WordPress MU before 2.8.1 allow remote attackers to obtain sensitive information via a direct request to wp-settings.php, which reveals the installation path in an error message.
CVE-2009-2431	WordPress 2.7.1 places the username of a post's author in an HTML comment, which allows remote attackers to obtain sensitive information by reading the HTML source.
CVE-2009-2336	The forgotten mail interface in WordPress and WordPress MU before 2.8.1 exhibits different behavior for a password request depending on whether the user account exists, which allows remote attackers to enumerate valid usernames. NOTE: the vendor reportedly disputes the significance of this issue, indicating that the behavior exists for "user convenience."
CVE-2009-2335	WordPress and WordPress MU before 2.8.1 exhibit different behavior for a failed login attempt depending on whether the user account exists, which allows remote attackers to enumerate valid usernames. NOTE: the vendor reportedly disputes the significance of this issue, indicating that the behavior exists for "user convenience."
CVE-2009-2334	wp-admin/admin.php in WordPress and WordPress MU before 2.8.1 does not require administrative authentication to access the configuration of a plugin, which allows remote attackers to specify a configuration file in the page parameter to obtain sensitive information or modify this file, as demonstrated by the (1) collapsing-archives/options.txt, (2) akismet/readme.txt, (3) related-ways-to-take-action/options.php, (4) wp-security-scan/securityscan.php, and (5) wp-ids/ids-admin.php files. NOTE: this can be leveraged for cross-site scripting (XSS) and denial of service.
CVE-2009-2396	PHP remote file inclusion vulnerability in template/album.php in DM Albums 1.9.2, as used standalone or as a WordPress plugin, allows remote attackers to execute arbitrary PHP code via a URL in the SECURITY_FILE parameter.
CVE-2009-2383	SQL injection vulnerability in BTE_RW_webajax.php in the Related Sites plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the guid parameter.
CVE-2009-2144	SQL injection vulnerability in the FireStats plugin before 1.6.2-stable for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors.
CVE-2009-2143	PHP remote file inclusion vulnerability in firestats-wordpress.php in the FireStats plugin before 1.6.2-stable for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the fs_javascript parameter.
CVE-2009-2122	SQL injection vulnerability in viewimg.php in the Paolo Palmonari Photoracer plugin 1.0 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
CVE-2008-6811	Unrestricted file upload vulnerability in image_processing.php in the e-Commerce Plugin 3.4 and earlier for Wordpress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in wp-content/plugins/wp-shopping-cart/.
CVE-2008-6767	wp-admin/upgrade.php in WordPress, probably 2.6.x, allows remote attackers to upgrade the application, and possibly cause a denial of service (application outage), via a direct request.
CVE-2008-6762	Open redirect vulnerability in wp-admin/upgrade.php in WordPress, probably 2.6.x, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the backto parameter.
CVE-2009-0968	SQL injection vulnerability in fmoblog.php in the fMoblog plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php. NOTE: some of these details are obtained from third party information.
CVE-2008-5752	Directory traversal vulnerability in getConfig.php in the Page Flip Image Gallery plugin 0.2.2 and earlier for WordPress, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the book_id parameter. NOTE: some of these details are obtained from third party information.
CVE-2008-5695	wp-admin/options.php in WordPress MU before 1.3.2, and WordPress 2.3.2 and earlier, does not properly validate requests to update an option, which allows remote authenticated users with manage_options and upload_files capabilities to execute arbitrary code by uploading a PHP script and adding this script's pathname to active_plugins.
CVE-2008-5278	Cross-site scripting (XSS) vulnerability in the self_link function in in the RSS Feed Generator (wp-includes/feed.php) for WordPress before 2.6.5 allows remote attackers to inject arbitrary web script or HTML via the Host header (HTTP_HOST variable).
CVE-2008-5113	WordPress 2.6.3 relies on the REQUEST superglobal array in certain dangerous situations, which makes it easier for remote attackers to conduct delayed and persistent cross-site request forgery (CSRF) attacks via crafted cookies, as demonstrated by attacks that (1) delete user accounts or (2) cause a denial of service (loss of application access). NOTE: this issue relies on the presence of an independent vulnerability that allows cookie injection.
CVE-2008-4769	Directory traversal vulnerability in the get_category_template function in wp-includes/theme.php in WordPress 2.3.3 and earlier, and 2.5, allows remote attackers to include and possibly execute arbitrary PHP files via the cat parameter in index.php. NOTE: some of these details are obtained from third party information.
CVE-2008-4734	Cross-site request forgery (CSRF) vulnerability in the wpcr_do_options_page function in WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to perform unauthorized actions as administrators via a request that sets the wpcr_hidden_form_input parameter.
CVE-2008-4733	Cross-site scripting (XSS) vulnerability in wpcommentremix.php in WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the (1) replytotext, (2) quotetext, (3) originallypostedby, (4) sep, (5) maxtags, (6) tagsep, (7) tagheadersep, (8) taglabel, and (9) tagheaderlabel parameters.

CVE-2008-4732	SQL injection vulnerability in ajax_comments.php in the WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to execute arbitrary SQL commands via the p parameter.
CVE-2008-4625	SQL injection vulnerability in stnl_iframe.php in the ShiftThis Newsletter (st_newsletter) plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the newsletter parameter, a different vector than CVE-2008-0683.
CVE-2008-4106	WordPress before 2.6.2 does not properly handle MySQL warnings about insertion of username strings that exceed the maximum column width of the user_login column, and does not properly handle space characters when comparing usernames, which allows remote attackers to change an arbitrary user's password to a random value by registering a similar username and then requesting a password reset, related to a "SQL column truncation vulnerability." NOTE: the attacker can discover the random password by also exploiting CVE-2008-4107.
CVE-2008-3747	The (1) get_edit_post_link and (2) get_edit_comment_link functions in wp-includes/link-template.php in WordPress before 2.6.1 do not force SSL communication in the intended situations, which might allow remote attackers to gain administrative access by sniffing the network for a cookie.
CVE-2008-3233	Cross-site scripting (XSS) vulnerability in WordPress before 2.6, SVN development versions only, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2008-2392	Unrestricted file upload vulnerability in WordPress 2.5.1 and earlier might allow remote authenticated administrators to upload and execute arbitrary PHP files via the Upload section in the Write Tabs area of the dashboard.
CVE-2008-2146	wp-includes/vars.php in Wordpress before 2.2.3 does not properly extract the current path from the PATH_INFO (\$PHP_SELF), which allows remote attackers to bypass intended access restrictions for certain pages.
CVE-2008-2068	Cross-site scripting (XSS) vulnerability in WordPress 2.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2008-1930	The cookie authentication method in WordPress 2.5 relies on a hash of a concatenated string containing USERNAME and EXPIRY_TIME, which allows remote attackers to forge cookies by registering a username that results in the same concatenated string, as demonstrated by registering usernames beginning with "admin" to obtain administrator privileges, aka a "cryptographic splicing" issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2007-6013.
CVE-2008-1982	SQL injection vulnerability in ss_load.php in the Spreadsheet (wpSS) 0.6 and earlier plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the ss_id parameter.
CVE-2008-1304	Multiple cross-site scripting (XSS) vulnerabilities in WordPress 2.3.2 allow remote attackers to inject arbitrary web script or HTML via the (1) inviteemail parameter in an invite action to wp-admin/users.php and the (2) to parameter in a sent action to wp-admin/invites.php.
CVE-2008-0664	The XML-RPC implementation (xmlrpc.php) in WordPress before 2.3.3, when registration is enabled, allows remote attackers to edit posts of other blog users via unknown vectors.
CVE-2008-0615	Directory traversal vulnerability in wp-admin/admin.php in the DMSGuestbook 1.8.0 and 1.7.0 plugin for WordPress allows remote authenticated users to read arbitrary files via a .. (dot dot) in the (1) folder and (2) file parameters.
CVE-2008-0616	SQL injection vulnerability in the administration panel in the DMSGuestbook 1.7.0 plugin for WordPress allows remote authenticated administrators to execute arbitrary SQL commands via unspecified vectors. NOTE: it is not clear whether this issue crosses privilege boundaries.
CVE-2008-0617	Multiple cross-site scripting (XSS) vulnerabilities in the DMSGuestbook 1.7.0 plugin for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) file parameter to wp-admin/admin.php, or the (2) messagefield parameter in the guestbook page, and the (3) title parameter in the messagearea.
CVE-2008-0618	Multiple cross-site scripting (XSS) vulnerabilities in the DMSGuestbook 1.8.0 and 1.7.0 plugin for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) gbname, (2) gbeamail, (3) gburl, and (4) gbmsg parameters to unspecified programs. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2008-0491	SQL injection vulnerability in fim_rss.php in the fGallery 2.4.1 plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the album parameter.
CVE-2007-6677	Cross-site scripting (XSS) vulnerability in Peter's Random Anti-Spam Image 0.2.4 and earlier plugin for WordPress allows remote attackers to inject arbitrary web script or HTML via the comment field in the comment form.
CVE-2008-0191	WordPress 2.2.x and 2.3.x allows remote attackers to obtain sensitive information via an invalid p parameter in an rss2 action to the default URI, which reveals the full path and the SQL database structure.
CVE-2008-0192	Multiple cross-site scripting (XSS) vulnerabilities in WordPress 2.0.9 and earlier allow remote attackers to inject arbitrary web script or HTML via the popuptitle parameter to (1) wp-admin/post.php or (2) wp-admin/page-new.php.
CVE-2008-0193	Cross-site scripting (XSS) vulnerability in wp-db-backup.php in WordPress 2.0.11 and earlier, and possibly 2.1.x through 2.3.x, allows remote attackers to inject arbitrary web script or HTML via the backup parameter in a wp-db-backup.php action to wp-admin/edit.php.

CVE-2008-0194	Directory traversal vulnerability in wp-db-backup.php in WordPress 2.0.3 and earlier allows remote attackers to read arbitrary files, delete arbitrary files, and cause a denial of service via a .. (dot dot) in the backup parameter in a wp-db-backup.php action to wp-admin/edit.php. NOTE: this might be the same as CVE-2006-5705.1.
CVE-2008-0195	WordPress 2.0.11 and earlier allows remote attackers to obtain sensitive information via an empty value of the page parameter to certain PHP scripts under wp-admin/, which reveals the path in various error messages.
CVE-2008-0196	Multiple directory traversal vulnerabilities in WordPress 2.0.11 and earlier allow remote attackers to read arbitrary files via a .. (dot dot) in (1) the page parameter to certain PHP scripts under wp-admin/ or (2) the import parameter to wp-admin/admin.php, as demonstrated by discovering the full path via a request for the \..\..\wp-config pathname; and allow remote attackers to modify arbitrary files via a .. (dot dot) in the file parameter to wp-admin/templates.php.
CVE-2008-0198	Multiple cross-site request forgery (CSRF) vulnerabilities in wp-contact-form/options-contactform.php in the WP-ContactForm 1.5 alpha and earlier plugin for WordPress allow remote attackers to perform actions as administrators via the (1) wpcf_question, (2) wpcf_success_msg, or (3) wpcf_error_msg parameter to wp-admin/admin.php.
CVE-2007-6318	SQL injection vulnerability in wp-includes/query.php in WordPress 2.3.1 and earlier allows remote attackers to execute arbitrary SQL commands via the s parameter, when DB_CHARSET is set to (1) Big5, (2) GBK, or possibly other character set encodings that support a "\\" in a multibyte character.
CVE-2007-6013	Wordpress 1.5 through 2.3.1 uses cookie values based on the MD5 hash of a password MD5 hash, which allows attackers to bypass authentication by obtaining the MD5 hash from the user database, then generating the authentication cookie from that hash.
CVE-2007-5800	Multiple PHP remote file inclusion vulnerabilities in the BackUpWordPress 0.4.2b and earlier plugin for WordPress allow remote attackers to execute arbitrary PHP code via a URL in the bkpwp_plugin_path parameter to (1) plugins/BackUp/Archive.php; and (2) Predicate.php, (3) Writer.php, (4) Reader.php, and other unspecified scripts under plugins/BackUp/Archive/.
CVE-2007-5710	Cross-site scripting (XSS) vulnerability in wp-admin/edit-post-rows.php in WordPress 2.3 allows remote attackers to inject arbitrary web script or HTML via the posts_columns array parameter.
CVE-2007-5105	Cross-site scripting (XSS) vulnerability in wp-register.php in WordPress 2.0 and 2.0.1 allows remote attackers to inject arbitrary web script or HTML via the user_email parameter.
CVE-2007-5106	Cross-site scripting (XSS) vulnerability in wp-register.php in WordPress 2.0 allows remote attackers to inject arbitrary web script or HTML via the user_login parameter.
CVE-2007-4893	wp-admin/admin-functions.php in Wordpress before 2.2.3 and Wordpress multi-user (MU) before 1.2.5a does not properly verify the unfiltered_html privilege, which allows remote attackers to conduct cross-site scripting (XSS) attacks via modified data to (1) post.php or (2) page.php with a no_filter field.
CVE-2007-4894	Multiple SQL injection vulnerabilities in Wordpress before 2.2.3 and Wordpress multi-user (MU) before 1.2.5a allow remote attackers to execute arbitrary SQL commands via the post_type parameter to the pingback.extensions.getPingbacks method in the XMLRPC interface, and other unspecified parameters related to "early database escaping" and missing validation of "query string like parameters."
CVE-2007-4165	Cross-site scripting (XSS) vulnerability in index.php in the Blue Memories theme 1.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter, possibly a related issue to CVE-2007-2757 and CVE-2007-4014. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2007-4153	Multiple cross-site scripting (XSS) vulnerabilities in WordPress 2.2.1 allow remote authenticated administrators to inject arbitrary web script or HTML via (1) the Options Database Table in the Admin Panel, accessed through options.php; or (2) the opml_url parameter to link-import.php. NOTE: this might not cross privilege boundaries in some configurations, since the Administrator role has the unfiltered_html capability.
CVE-2007-4154	SQL injection vulnerability in options.php in WordPress 2.2.1 allows remote authenticated administrators to execute arbitrary SQL commands via the page_options parameter to (1) options-general.php, (2) options-writing.php, (3) options-reading.php, (4) options-discussion.php, (5) options-privacy.php, (6) options-permalink.php, (7) options-misc.php, and possibly other unspecified components.
CVE-2007-4139	Cross-site scripting (XSS) vulnerability in the Temporary Uploads editing functionality (wp-admin/includes/upload.php) in WordPress 2.2.1, allows remote attackers to inject arbitrary web script or HTML via the style parameter to wp-admin/upload.php.
CVE-2007-3639	WordPress before 2.2.2 allows remote attackers to redirect visitors to other websites and potentially obtain sensitive information via (1) the _wp_http_referer parameter to wp-pass.php, related to the wp_get_referer function in wp-includes/functions.php; and possibly other vectors related to (2) wp-includes/pluggable.php and (3) the wp_nonce_ays function in wp-includes/functions.php.
CVE-2007-3543	Unrestricted file upload vulnerability in WordPress before 2.2.1 and WordPress MU before 1.2.3 allows remote authenticated users to upload and execute arbitrary PHP code by making a post that specifies a .php filename in the _wp_attached_file metadata field; and then sending this file's content, along with its post_ID value, to (1) wp-app.php or (2) app.php.
CVE-2007-3544	Unrestricted file upload vulnerability in (1) wp-app.php and (2) app.php in WordPress 2.2.1 and WordPress MU 1.2.3 allows remote authenticated users to upload and execute arbitrary PHP code via unspecified vectors, possibly

	related to the wp_postmeta table and the use of custom fields in normal (non-attachment) posts. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2007-3543.
CVE-2007-3238	Cross-site scripting (XSS) vulnerability in functions.php in the default theme in WordPress 2.2 allows remote authenticated administrators to inject arbitrary web script or HTML via the PATH_INFO (REQUEST_URI) to wp-admin/themes.php, a different vulnerability than CVE-2007-1622. NOTE: this might not cross privilege boundaries in some configurations, since the Administrator role has the unfiltered_html capability.
CVE-2007-3239	Cross-site scripting (XSS) vulnerability in searchform.php in the AndyBlue theme before 20070607 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PHP_SELF portion of a URI to index.php. NOTE: this can be leveraged for PHP code execution in an administrative session.
CVE-2007-3240	Cross-site scripting (XSS) vulnerability in 404.php in the Vistered-Little theme for WordPress allows remote attackers to inject arbitrary web script or HTML via the URI (REQUEST_URI) that accesses index.php. NOTE: this can be leveraged for PHP code execution in an administrative session.
CVE-2007-3241	Cross-site scripting (XSS) vulnerability in blogroll.php in the cordobo-green-park theme for WordPress allows remote attackers to inject arbitrary web script or HTML via the PHP_SELF portion of a URI.
CVE-2007-3140	SQL injection vulnerability in xmlrpc.php in WordPress 2.2 allows remote authenticated users to execute arbitrary SQL commands via a parameter value in an XML RPC wp.suggestCategories methodCall, a different vector than CVE-2007-1897.
CVE-2007-2821	SQL injection vulnerability in wp-admin/admin-ajax.php in WordPress before 2.2 allows remote attackers to execute arbitrary SQL commands via the cookie parameter.
CVE-2007-2627	Cross-site scripting (XSS) vulnerability in sidebar.php in WordPress, when custom 404 pages that call get_sidebar are used, allows remote attackers to inject arbitrary web script or HTML via the query string (PHP_SELF), a different vulnerability than CVE-2007-1622.
CVE-2007-1893	xmlrpc (xmlrpc.php) in WordPress 2.1.2, and probably earlier, allows remote authenticated users with the contributor role to bypass intended access restrictions and invoke the publish_posts functionality, which can be used to "publish a previously saved post."
CVE-2007-1894	Cross-site scripting (XSS) vulnerability in wp-includes/general-template.php in WordPress before 20070309 allows remote attackers to inject arbitrary web script or HTML via the year parameter in the wp_title function.
CVE-2007-1897	SQL injection vulnerability in xmlrpc (xmlrpc.php) in WordPress 2.1.2, and probably earlier, allows remote authenticated users to execute arbitrary SQL commands via a string parameter value in an XML RPC mt.setPostCategories method call, related to the post_id variable.
CVE-2007-1732	** DISPUTED ** Cross-site scripting (XSS) vulnerability in an mt import in wp-admin/admin.php in WordPress 2.1.2 allows remote authenticated administrators to inject arbitrary web script or HTML via the demo parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. NOTE: another researcher disputes this issue, stating that this is legitimate functionality for administrators. However, it has been patched by at least one vendor.
CVE-2007-1622	Cross-site scripting (XSS) vulnerability in wp-admin/vars.php in WordPress before 2.0.10 RC2, and before 2.1.3 RC2 in the 2.1 series, allows remote authenticated users with theme privileges to inject arbitrary web script or HTML via the PATH_INFO in the administration interface, related to loose regular expression processing of PHP_SELF.
CVE-2007-1599	wp-login.php in WordPress allows remote attackers to redirect authenticated users to other websites and potentially obtain sensitive information via the redirect_to parameter.
CVE-2007-1409	WordPress allows remote attackers to obtain sensitive information via a direct request for wp-admin/admin-functions.php, which reveals the path in an error message.
CVE-2007-1277	WordPress 2.1.1, as downloaded from some official distribution sites during February and March 2007, contains an externally introduced backdoor that allows remote attackers to execute arbitrary commands via (1) an eval injection vulnerability in the ix parameter to wp-includes/feed.php, and (2) an untrusted passthru call in the iz parameter to wp-includes/theme.php.
CVE-2007-1244	Cross-site request forgery (CSRF) vulnerability in the AdminPanel in WordPress 2.1.1 and earlier allows remote attackers to perform privileged actions as administrators, as demonstrated using the delete action in wp-admin/post.php. NOTE: this issue can be leveraged to perform cross-site scripting (XSS) attacks and steal cookies via the post parameter.
CVE-2007-1230	Multiple cross-site scripting (XSS) vulnerabilities in wp-includes/functions.php in WordPress before 2.1.2-alpha allow remote attackers to inject arbitrary web script or HTML via (1) the Referer HTTP header or (2) the URI, a different vulnerability than CVE-2007-1049.
CVE-2007-1049	Cross-site scripting (XSS) vulnerability in the wp_explain_nonce function in the nonce AYS functionality (wp-includes/functions.php) for WordPress 2.0 before 2.0.9 and 2.1 before 2.1.1 allows remote attackers to inject arbitrary web script or HTML via the file parameter to wp-admin/templates.php, and possibly other vectors involving the action variable.
CVE-2007-0539	The wp_remote_fopen function in WordPress before 2.1 allows remote attackers to cause a denial of service (bandwidth or thread consumption) via pingback service calls with a source URI that corresponds to a large file, which triggers a long download session without a timeout constraint.

CVE-2007-0540	WordPress allows remote attackers to cause a denial of service (bandwidth or thread consumption) via pingback service calls with a source URI that corresponds to a file with a binary content type, which is downloaded even though it cannot contain usable pingback data.
CVE-2007-0541	WordPress allows remote attackers to determine the existence of arbitrary files, and possibly read portions of certain files, via pingback service calls with a source URI that corresponds to a local pathname, which triggers different fault codes for existing and non-existing files, and in certain configurations causes a brief file excerpt to be published as a blog comment.
CVE-2007-0262	WordPress 2.0.6, and 2.1Alpha 3 (SVN:4662), does not properly verify that the m parameter value has the string data type, which allows remote attackers to obtain sensitive information via an invalid m[] parameter, as demonstrated by obtaining the path, and obtaining certain SQL information such as the table prefix.
CVE-2007-0233	wp-trackback.php in WordPress 2.0.6 and earlier does not properly unset variables when the input data includes a numeric parameter with a value matching an alphanumeric parameter's hash value, which allows remote attackers to execute arbitrary SQL commands via the tb_id parameter. NOTE: it could be argued that this vulnerability is due to a bug in the unset PHP command (CVE-2006-3017) and the proper fix should be in PHP; if so, then this should not be treated as a vulnerability in WordPress.
CVE-2007-0106	Cross-site scripting (XSS) vulnerability in the CSRF protection scheme in WordPress before 2.0.6 allows remote attackers to inject arbitrary web script or HTML via a CSRF attack with an invalid token and quote characters or HTML tags in URL variable names, which are not properly handled when WordPress generates a new link to verify the request.
CVE-2007-0107	WordPress before 2.0.6, when mbstring is enabled for PHP, decodes alternate character sets after escaping the SQL query, which allows remote attackers to bypass SQL injection protection schemes and execute arbitrary SQL commands via multibyte charsets, as demonstrated using UTF-7.
CVE-2007-0109	wp-login.php in WordPress 2.0.5 and earlier displays different error messages if a user exists or not, which allows remote attackers to obtain sensitive information and facilitates brute force attacks.
CVE-2006-6808	Cross-site scripting (XSS) vulnerability in wp-admin/templates.php in WordPress 2.0.5 allows remote attackers to inject arbitrary web script or HTML via the file parameter. NOTE: some sources have reported this as a vulnerability in the get_file_description function in wp-admin/admin-functions.php.
CVE-2006-6016	wp-admin/user-edit.php in WordPress before 2.0.5 allows remote authenticated users to read the metadata of an arbitrary user via a modified user_id parameter.
CVE-2006-6017	WordPress before 2.0.5 does not properly store a profile containing a string representation of a serialized object, which allows remote authenticated users to cause a denial of service (application crash) via a string that represents a (1) malformed or (2) large serialized object, because the object triggers automatic unserialization for display.
CVE-2006-5705	Multiple directory traversal vulnerabilities in plugins/wp-db-backup.php in WordPress before 2.0.5 allow remote authenticated users to read or overwrite arbitrary files via directory traversal sequences in the (1) backup and (2) fragment parameters in a GET request.
CVE-2006-4743	WordPress 2.0.2 through 2.0.5 allows remote attackers to obtain sensitive information via a direct request for (1) 404.php, (2) akismet.php, (3) archive.php, (4) archives.php, (5) attachment.php, (6) blogger.php, (7) comments.php, (8) comments-popup.php, (9) dotclear.php, (10) footer.php, (11) functions.php, (12) header.php, (13) hello.php, (14) wp-content/themes/default/index.php, (15) links.php, (16) livejournal.php, (17) mt.php, (18) page.php, (19) rss.php, (20) searchform.php, (21) search.php, (22) sidebar.php, (23) single.php, (24) textpattern.php, (25) upgrade-functions.php, (26) upgrade-schema.php, or (27) wp-db-backup.php, which reveal the path in various error messages. NOTE: another researcher has disputed the details of this report, stating that version 2.0.5 does not exist. NOTE: the admin-footer.php, admin-functions.php, default-filters.php, edit-form-advanced.php, edit-link-form.php, edit-page-form.php, kses.php, locale.php, rss-functions.php, template-loader.php, and wp-db.php vectors are already covered by CVE-2006-0986. The edit-form-comment.php, vars.php, and wp-settings.php vectors are already covered by CVE-2005-4463. The menu-header.php vector is already covered by CVE-2005-2110.
CVE-2006-4028	Multiple unspecified vulnerabilities in WordPress before 2.0.4 have unknown impact and remote attack vectors. NOTE: due to lack of details, it is not clear how these issues are different from CVE-2006-3389 and CVE-2006-3390, although it is likely that 2.0.4 addresses an unspecified issue related to "Anyone can register" functionality (user registration for guests).
CVE-2006-3389	index.php in WordPress 2.0.3 allows remote attackers to obtain sensitive information, such as SQL table prefixes, via an invalid paged parameter, which displays the information in an SQL error message. NOTE: this issue has been disputed by a third party who states that the issue does not leak any target-specific information.
CVE-2006-3390	WordPress 2.0.3 allows remote attackers to obtain the installation path via a direct request to various files, such as those in the (1) wp-admin, (2) wp-content, and (3) wp-includes directories, possibly due to uninitialized variables.
CVE-2006-2702	vars.php in WordPress 2.0.2, possibly when running on Mac OS X, allows remote attackers to spoof their IP address via a PC_REMOTE_ADDR HTTP header, which vars.php uses to redefine \$_SERVER['REMOTE_ADDR'].
CVE-2006-2667	Direct static code injection vulnerability in WordPress 2.0.2 and earlier allows remote attackers to execute arbitrary commands by inserting a carriage return and PHP code when updating a profile, which is appended after a special

	comment sequence into files in (1) wp-content/cache/userlogins/ (2) wp-content/cache/users/ which are later included by cache.php, as demonstrated using the displayname argument.
CVE-2006-1796	Cross-site scripting (XSS) vulnerability in the paging links functionality in template-functions-links.php in Wordpress 1.5.2, and possibly other versions before 2.0.1, allows remote attackers to inject arbitrary web script or HTML to Internet Explorer users via the request URI ( <code>\$_SERVER['REQUEST_URI']</code> ).
CVE-2006-1263	Multiple "unannounced" cross-site scripting (XSS) vulnerabilities in WordPress before 2.0.2 allow remote attackers to inject arbitrary web script or HTML via unknown attack vectors.
CVE-2006-1012	SQL injection vulnerability in WordPress 1.5.2, and possibly other versions before 2.0, allows remote attackers to execute arbitrary SQL commands via the User-Agent field in an HTTP header for a comment.
CVE-2006-0985	Multiple cross-site scripting (XSS) vulnerabilities in the "post comment" functionality of WordPress 2.0.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) name, (2) website, and (3) comment parameters.
CVE-2006-0986	WordPress 2.0.1 and earlier allows remote attackers to obtain sensitive information via a direct request to (1) default-filters.php, (2) template-loader.php, (3) rss-functions.php, (4) locale.php, (5) wp-db.php, and (6) kses.php in the wp-includes/ directory; and (7) edit-form-advanced.php, (8) admin-functions.php, (9) edit-link-form.php, (10) edit-page-form.php, (11) admin-footer.php, and (12) menu.php in the wp-admin directory; and possibly (13) list directory contents of the wp-includes directory. NOTE: the vars.php, edit-form.php, wp-settings.php, and edit-form-comment.php vectors are already covered by CVE-2005-4463. The menu-header.php vector is already covered by CVE-2005-2110. Other vectors might be covered by CVE-2005-1688. NOTE: if the typical installation of WordPress does not list any site-specific files to wp-includes, then vector [13] is not an exposure.
CVE-2006-0733	** DISPUTED ** Cross-site scripting (XSS) vulnerability in WordPress 2.0.0 allows remote attackers to inject arbitrary web script or HTML via scriptable attributes such as (1) onfocus and (2) onblur in the "author's website" field. NOTE: followup comments to the researcher's web log suggest that this issue is only exploitable by the same user who injects the XSS, so this might not be a vulnerability.
CVE-2005-4463	WordPress before 1.5.2 allows remote attackers to obtain sensitive information via a direct request to (1) wp-includes/vars.php, (2) wp-content/plugins/hello.php, (3) wp-admin/upgrade-functions.php, (4) wp-admin/edit-form.php, (5) wp-settings.php, and (6) wp-admin/edit-form-comment.php, which leaks the path in an error message related to undefined functions or failed includes. NOTE: the wp-admin/menu-header.php vector is already covered by CVE-2005-2110. NOTE: the vars.php, edit-form.php, wp-settings.php, and edit-form-comment.php vectors were also reported to affect WordPress 2.0.1.
CVE-2005-2612	Direct code injection vulnerability in WordPress 1.5.1.3 and earlier allows remote attackers to execute arbitrary PHP code via the cache_lastpostdate[server] cookie.
CVE-2005-2107	Multiple cross-site scripting (XSS) vulnerabilities in post.php in WordPress 1.5.1.2 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) p or (2) comment parameter.
CVE-2005-2108	SQL injection vulnerability in XMLRPC server in WordPress 1.5.1.2 and earlier allows remote attackers to execute arbitrary SQL commands via input that is not filtered in the <code>HTTP_RAW_POST_DATA</code> variable, which stores the data in an XML file.
CVE-2005-2109	wp-login.php in WordPress 1.5.1.2 and earlier allows remote attackers to change the content of the forgotten password e-mail message via the message variable, which is not initialized before use.
CVE-2005-2110	WordPress 1.5.1.2 and earlier allows remote attackers to obtain sensitive information via (1) a direct request to menu-header.php or a "1" value in the feed parameter to (2) wp-atom.php, (3) wp-rss.php, or (4) wp-rss2.php, which reveal the path in an error message. NOTE: vector [1] was later reported to also affect WordPress 2.0.1.
CVE-2005-1810	SQL injection vulnerability in template-functions-category.php in WordPress 1.5.1 allows remote attackers to execute arbitrary SQL commands via the \$cat_ID variable, as demonstrated using the cat parameter to index.php.
CVE-2005-1687	SQL injection vulnerability in wp-trackback.php in Wordpress 1.5 and earlier allows remote attackers to execute arbitrary SQL commands via the tb_id parameter.
CVE-2005-1688	Wordpress 1.5 and earlier allows remote attackers to obtain sensitive information via a direct request to files in (1) wp-content/themes/, (2) wp-includes/, or (3) wp-admin/, which reveal the path in an error message.
CVE-2005-1102	Multiple cross-site scripting (XSS) vulnerabilities in template-functions-post.php in WordPress 1.5 and earlier allow remote attackers to execute arbitrary commands via the (1) content or (2) title of the post.
CVE-2004-1559	Multiple cross-site scripting (XSS) vulnerabilities in Wordpress 1.2 allow remote attackers to inject arbitrary web script or HTML via the (1) redirect_to, text, popupurl, or popuptitle parameters to wp-login.php, (2) redirect_url parameter to admin-header.php, (3) popuptitle, popupurl, content, or post_title parameters to bookmarklet.php, (4) cat_ID parameter to categories.php, (5) s parameter to edit.php, or (6) s or mode parameter to edit-comments.php.
CVE-2004-1584	CRLF injection vulnerability in wp-login.php in WordPress 1.2 allows remote attackers to perform HTTP Response Splitting attacks to modify expected HTML content from the server via the text parameter.

## Filtered CVEs

### Chromium CVEs

CVE ID	Keword-based	Component-based	File-based
CVE-2009-3932	X	N/A	N/A
CVE-2010-0649	N/A	N/A	X
CVE-2010-0657	X	N/A	N/A
CVE-2010-1228	N/A	N/A	X
CVE-2010-1229	N/A	N/A	X
CVE-2010-1851	X	N/A	N/A
CVE-2010-2108	X	N/A	N/A
CVE-2010-2110	X	N/A	N/A
CVE-2010-3116	X	N/A	N/A
CVE-2010-3250	X	X	X
CVE-2010-3258	N/A	N/A	X
CVE-2010-3417	X	X	X
CVE-2010-4491	X	N/A	N/A
CVE-2010-4575	X	X	N/A
CVE-2011-0470	X	N/A	N/A
CVE-2011-0472	N/A	X	N/A
CVE-2011-0475	N/A	X	N/A
CVE-2011-0476	N/A	X	N/A
CVE-2011-0479	X	N/A	N/A
CVE-2011-0481	N/A	X	N/A
CVE-2011-0779	X	X	N/A
CVE-2011-0984	X	N/A	N/A
CVE-2011-1123	X	X	N/A
CVE-2011-1124	X	X	X
CVE-2011-1304	X	N/A	X
CVE-2011-1434	N/A	X	N/A
CVE-2011-1435	X	N/A	X
CVE-2011-1443	N/A	N/A	X
CVE-2011-1444	N/A	N/A	X
CVE-2011-1450	N/A	X	N/A
CVE-2011-1812	X	X	X
CVE-2011-1813	X	N/A	N/A
CVE-2011-1815	X	X	X
CVE-2011-1819	X	X	X
CVE-2011-2345	N/A	X	X
CVE-2011-2358	X	X	X
CVE-2011-2783	X	X	N/A
CVE-2011-2785	X	X	X
CVE-2011-2787	N/A	X	N/A

CVE-2011-2789	X	X	X
CVE-2011-2836	X	X	X
CVE-2011-2838	X	N/A	X
CVE-2011-2853	X	X	X
CVE-2011-3015	N/A	X	N/A
CVE-2011-3046	X	N/A	N/A
CVE-2011-3047	X	N/A	N/A
CVE-2011-3049	X	X	X
CVE-2011-3055	X	X	N/A
CVE-2011-3079	N/A	N/A	X
CVE-2011-3080	N/A	X	X
CVE-2011-3098	X	X	X
CVE-2011-3107	X	N/A	N/A
CVE-2011-3875	N/A	N/A	X
CVE-2011-3881	X	N/A	N/A
CVE-2011-3888	X	N/A	N/A
CVE-2011-3898	N/A	N/A	X
CVE-2011-3956	X	X	X
CVE-2011-3961	N/A	N/A	X
CVE-2012-2816	N/A	N/A	X
CVE-2012-2853	N/A	X	N/A
CVE-2012-2869	N/A	X	X
CVE-2012-2877	X	X	N/A
CVE-2012-2878	X	X	N/A
CVE-2012-2880	X	N/A	X
CVE-2012-2881	X	N/A	N/A
CVE-2012-5111	X	N/A	N/A
CVE-2012-5125	X	X	N/A
CVE-2012-5126	X	N/A	N/A
CVE-2012-5140	N/A	X	X
CVE-2012-5141	X	N/A	N/A
CVE-2012-5143	N/A	X	X
CVE-2012-5156	N/A	X	N/A
CVE-2013-0828	N/A	X	N/A
CVE-2013-0830	N/A	N/A	X
CVE-2013-0831	X	N/A	X
CVE-2013-0837	X	X	N/A
CVE-2013-0842	N/A	N/A	X
CVE-2013-0892	N/A	N/A	X
CVE-2013-0896	X	X	N/A
CVE-2013-0897	N/A	X	N/A
CVE-2013-0898	N/A	X	N/A
CVE-2013-0908	X	N/A	N/A
CVE-2013-0910	X	N/A	X

CVE-2013-0917	N/A	X	N/A
CVE-2013-0919	X	X	N/A
CVE-2013-0920	X	X	N/A
CVE-2013-0923	X	X	N/A
CVE-2013-0924	X	X	N/A
CVE-2013-0925	X	X	N/A
CVE-2013-2836	N/A	X	X
CVE-2013-2841	N/A	X	X
CVE-2013-2854	N/A	N/A	X
CVE-2013-2866	X	X	X
CVE-2013-2868	X	X	X
CVE-2013-2872	N/A	N/A	X
CVE-2013-2876	X	X	N/A
CVE-2013-2880	N/A	X	X
CVE-2013-2912	X	N/A	X
CVE-2013-2931	N/A	X	N/A
CVE-2013-6644	N/A	X	N/A
CVE-2013-6645	N/A	X	N/A
CVE-2013-6652	N/A	N/A	X
CVE-2013-6658	X	N/A	N/A
CVE-2013-6661	N/A	X	N/A
CVE-2013-6666	N/A	X	X
CVE-2014-1715	N/A	X	N/A
CVE-2014-1728	N/A	X	N/A
CVE-2014-1733	N/A	N/A	X
CVE-2014-3170	X	X	N/A
CVE-2014-3172	X	X	N/A
CVE-2014-3175	N/A	X	N/A
CVE-2014-3176	X	N/A	N/A
CVE-2014-3177	X	N/A	N/A
CVE-2014-3189	N/A	X	N/A
CVE-2014-3198	N/A	X	N/A
CVE-2014-7900	N/A	X	N/A
CVE-2014-7901	N/A	X	N/A
CVE-2014-7903	N/A	X	N/A
CVE-2014-7906	X	N/A	N/A
CVE-2014-7935	N/A	X	N/A
CVE-2014-7944	N/A	X	N/A
CVE-2014-7945	N/A	X	N/A
CVE-2014-7948	N/A	X	N/A
CVE-2015-1205	N/A	X	N/A
CVE-2015-1226	X	X	N/A
CVE-2015-1231	N/A	X	N/A
CVE-2015-1241	N/A	N/A	X
CVE-2015-1245	N/A	X	N/A
CVE-2015-1265	N/A	X	N/A
CVE-2015-1267	N/A	X	N/A
CVE-2015-1271	N/A	X	N/A
CVE-2015-1278	N/A	X	N/A

CVE-2015-1279	N/A	X	N/A
CVE-2015-1281	N/A	X	N/A
CVE-2015-1282	N/A	X	N/A
CVE-2015-1286	X	N/A	N/A
CVE-2015-1297	X	X	N/A
CVE-2015-1298	X	X	N/A
CVE-2015-1302	X	X	N/A
CVE-2015-1359	N/A	X	N/A
CVE-2015-3335	N/A	N/A	X
CVE-2015-6583	N/A	X	N/A
CVE-2015-6758	N/A	X	N/A
CVE-2015-6765	N/A	X	N/A
CVE-2015-6766	N/A	X	N/A
CVE-2015-6767	N/A	X	N/A
CVE-2015-6772	X	N/A	N/A
CVE-2015-6774	X	N/A	N/A
CVE-2015-6775	N/A	X	N/A
CVE-2015-6776	N/A	X	N/A
CVE-2015-6778	N/A	X	N/A
CVE-2015-6779	N/A	X	N/A
CVE-2015-6786	N/A	N/A	X
CVE-2015-6788	X	N/A	N/A
CVE-2016-1613	N/A	X	N/A
CVE-2016-1619	N/A	X	N/A
CVE-2016-1620	N/A	X	N/A
CVE-2016-1622	X	N/A	N/A
CVE-2016-1626	N/A	X	N/A
CVE-2016-1627	X	N/A	N/A
CVE-2016-1628	N/A	X	N/A
CVE-2016-1631	X	X	X
CVE-2016-1632	X	N/A	N/A
CVE-2016-1635	X	X	N/A
CVE-2016-1638	X	X	X
CVE-2016-1639	X	X	N/A
CVE-2016-1640	X	X	N/A
CVE-2016-1648	X	N/A	N/A
CVE-2016-1650	X	X	N/A

#### Firefox CVEs

CVE ID	Keword-based	Component-based	File-based
CVE-2004-0762	X	N/A	X
CVE-2004-1639	X	N/A	N/A
CVE-2004-1753	X	X	N/A
CVE-2004-2227	X	N/A	N/A
CVE-2005-0142	N/A	N/A	X
CVE-2005-0143	N/A	N/A	X
CVE-2005-0230	X	N/A	N/A
CVE-2005-0232	X	X	N/A

CVE-2005-0399	X	N/A	N/A
CVE-2005-0527	X	N/A	N/A
CVE-2005-0578	X	N/A	N/A
CVE-2005-0586	X	N/A	N/A
CVE-2005-0588	N/A	N/A	X
CVE-2005-0590	N/A	X	X
CVE-2005-0752	X	N/A	N/A
CVE-2005-1156	X	N/A	N/A
CVE-2005-1157	X	N/A	N/A
CVE-2005-1159	N/A	X	X
CVE-2005-1476	N/A	N/A	X
CVE-2005-1477	X	N/A	X
CVE-2005-1576	X	N/A	N/A
CVE-2005-2260	N/A	N/A	X
CVE-2005-2263	N/A	X	X
CVE-2005-2265	N/A	X	N/A
CVE-2006-1273	X	N/A	N/A
CVE-2006-1736	X	N/A	N/A
CVE-2006-2538	X	N/A	N/A
CVE-2006-2784	X	N/A	N/A
CVE-2006-3731	X	N/A	N/A
CVE-2006-6499	X	N/A	N/A
CVE-2006-6585	X	N/A	N/A
CVE-2007-0896	X	N/A	N/A
CVE-2007-3285	X	N/A	N/A
CVE-2007-3844	X	N/A	N/A
CVE-2007-3845	X	N/A	X
CVE-2007-4013	X	N/A	N/A
CVE-2007-4041	N/A	N/A	X
CVE-2007-5045	N/A	N/A	X
CVE-2007-5337	N/A	N/A	X
CVE-2007-5459	X	N/A	N/A
CVE-2008-0367	N/A	N/A	X
CVE-2008-0415	N/A	N/A	X
CVE-2008-0418	X	N/A	N/A
CVE-2008-0592	N/A	N/A	X
CVE-2008-1240	X	N/A	N/A
CVE-2008-2399	X	N/A	N/A
CVE-2008-2803	X	N/A	N/A
CVE-2008-2806	X	X	N/A
CVE-2008-2807	X	N/A	N/A
CVE-2008-4062	N/A	X	N/A
CVE-2008-4063	X	N/A	N/A

CVE-2008-5013	X	X	N/A
CVE-2008-5021	N/A	N/A	X
CVE-2008-5022	N/A	N/A	X
CVE-2008-5052	X	N/A	N/A
CVE-2008-5506	N/A	N/A	X
CVE-2008-5697	X	N/A	N/A
CVE-2009-0356	X	N/A	N/A
CVE-2009-0357	N/A	N/A	X
CVE-2009-1310	X	N/A	N/A
CVE-2009-1392	X	N/A	N/A
CVE-2009-1837	X	X	N/A
CVE-2009-2011	X	N/A	N/A
CVE-2009-2467	X	X	N/A
CVE-2009-2665	X	N/A	N/A
CVE-2009-3274	N/A	N/A	X
CVE-2009-3376	X	N/A	X
CVE-2009-3478	X	N/A	N/A
CVE-2009-3983	N/A	N/A	X
CVE-2009-4100	X	N/A	N/A
CVE-2009-4101	X	N/A	N/A
CVE-2009-4102	X	N/A	N/A
CVE-2009-4127	X	N/A	N/A
CVE-2010-0159	N/A	N/A	X
CVE-2010-0167	X	X	N/A
CVE-2010-0168	X	N/A	N/A
CVE-2010-0170	X	N/A	N/A
CVE-2010-0177	X	X	N/A
CVE-2010-0179	X	N/A	N/A
CVE-2010-1198	X	X	N/A
CVE-2010-1214	X	X	N/A
CVE-2010-1585	X	N/A	N/A
CVE-2010-2755	X	X	N/A
CVE-2010-2767	X	N/A	N/A
CVE-2010-2792	X	N/A	N/A
CVE-2010-2794	X	N/A	N/A
CVE-2010-3181	N/A	N/A	X
CVE-2010-3773	X	N/A	N/A
CVE-2011-0012	X	N/A	N/A
CVE-2011-0059	X	X	N/A
CVE-2011-0076	X	X	N/A
CVE-2011-0081	N/A	X	N/A
CVE-2011-0341	X	N/A	N/A
CVE-2011-1179	X	N/A	N/A

CVE-2011-2362	N/A	N/A	X
CVE-2011-2370	X	X	X
CVE-2011-2990	N/A	X	X
CVE-2011-2995	N/A	N/A	X
CVE-2011-2996	X	N/A	N/A
CVE-2011-3001	X	N/A	X
CVE-2011-3004	X	N/A	N/A
CVE-2011-3384	X	N/A	N/A
CVE-2011-3647	X	N/A	N/A
CVE-2011-3664	X	X	X
CVE-2012-0446	X	N/A	N/A
CVE-2012-0461	N/A	X	X
CVE-2012-1956	X	N/A	X
CVE-2012-3960	X	N/A	X
CVE-2012-3973	X	N/A	N/A
CVE-2012-3975	X	N/A	N/A
CVE-2012-3987	N/A	N/A	X
CVE-2012-3991	N/A	N/A	X
CVE-2012-3994	X	N/A	N/A
CVE-2012-4194	X	N/A	N/A
CVE-2012-4195	X	N/A	N/A
CVE-2012-4201	X	N/A	N/A
CVE-2012-4205	X	N/A	N/A
CVE-2012-4209	X	N/A	N/A
CVE-2012-5354	X	N/A	N/A
CVE-2013-0747	X	X	X
CVE-2013-0756	N/A	N/A	X
CVE-2013-0758	X	X	X
CVE-2013-0760	N/A	N/A	X
CVE-2013-0779	N/A	N/A	X
CVE-2013-0790	X	X	X
CVE-2013-0791	X	N/A	N/A
CVE-2013-0798	X	N/A	N/A
CVE-2013-1679	X	X	X
CVE-2013-1713	X	X	X
CVE-2013-1717	N/A	X	X
CVE-2013-5598	N/A	N/A	X
CVE-2013-6853	X	N/A	N/A
CVE-2014-1485	N/A	N/A	X
CVE-2014-1509	X	N/A	N/A
CVE-2014-1513	N/A	N/A	X
CVE-2014-1514	N/A	N/A	X
CVE-2014-1519	N/A	N/A	X
CVE-2014-1539	N/A	X	N/A

CVE-2014-1595	N/A	N/A	X
CVE-2014-8642	X	N/A	N/A
CVE-2014-8643	X	N/A	N/A
CVE-2015-0812	X	X	X
CVE-2015-0813	X	N/A	N/A
CVE-2015-2706	X	X	X
CVE-2015-2709	N/A	X	N/A
CVE-2015-2741	X	N/A	N/A
CVE-2015-4495	N/A	N/A	X
CVE-2015-4498	X	X	X
CVE-2015-4503	X	N/A	N/A
CVE-2015-7187	X	N/A	N/A
CVE-2015-7196	X	X	X
CVE-2015-7205	X	N/A	N/A
CVE-2015-7223	X	X	X
CVE-2016-1948	X	N/A	N/A
CVE-2016-1949	X	N/A	X
CVE-2016-1966	X	X	X

#### OfBiz CVEs

CVE ID	Keword-based	Component-based	File-based
CVE-2017-15714	X	N/A	N/A

#### OpenMRS CVEs

CVE ID	Keword-based	Component-based	File-based
CVE-2017-12796	X	N/A	N/A

#### Pidgin CVEs

CVE ID	Keword-based	Component-based	File-based
CVE-2008-3532	X	X	N/A
CVE-2009-2703	X	N/A	N/A
CVE-2009-3083	X	N/A	N/A
CVE-2009-3084	X	N/A	N/A
CVE-2009-3085	X	N/A	N/A
CVE-2009-3615	X	N/A	N/A
CVE-2010-0013	X	N/A	N/A
CVE-2010-0277	X	N/A	N/A
CVE-2010-1624	X	N/A	N/A
CVE-2010-2528	X	N/A	N/A
CVE-2010-3088	X	N/A	N/A

CVE-2010-3711	X	N/A	X
CVE-2010-4528	X	N/A	N/A
CVE-2011-1091	X	N/A	N/A
CVE-2011-2943	X	N/A	N/A
CVE-2011-3184	X	N/A	N/A
CVE-2011-3594	X	N/A	N/A
CVE-2011-4601	X	N/A	N/A
CVE-2011-4602	X	N/A	N/A
CVE-2011-4603	X	N/A	N/A
CVE-2012-1178	X	N/A	N/A
CVE-2012-2318	X	N/A	N/A
CVE-2012-2369	X	N/A	N/A
CVE-2012-3374	X	N/A	N/A
CVE-2012-6152	X	N/A	N/A
CVE-2013-0271	X	N/A	N/A
CVE-2013-0272	X	N/A	N/A
CVE-2013-0273	X	N/A	N/A
CVE-2013-6483	X	N/A	N/A
CVE-2014-0020	X	N/A	N/A
CVE-2014-3694	X	N/A	X
CVE-2014-3695	X	N/A	N/A
CVE-2014-3696	X	N/A	N/A
CVE-2014-3698	X	N/A	N/A

### Thunderbird CVEs

CVE ID	Keword-based	Component-based	File-based
CVE-2004-0762	X	N/A	X
CVE-2004-0906	X	X	X
CVE-2004-0907	N/A	N/A	X
CVE-2005-0142	N/A	N/A	X
CVE-2005-0148	N/A	N/A	X
CVE-2005-0149	N/A	N/A	X
CVE-2005-0399	X	N/A	N/A
CVE-2005-0590	N/A	X	X
CVE-2006-0236	X	N/A	X
CVE-2006-1736	X	N/A	N/A
CVE-2006-3809	N/A	N/A	X
CVE-2006-4571	X	N/A	X
CVE-2006-6499	X	N/A	N/A
CVE-2007-3844	X	N/A	N/A
CVE-2007-3845	X	N/A	X
CVE-2007-4841	N/A	N/A	X
CVE-2008-0415	N/A	N/A	X

CVE-2008-0418	X	N/A	N/A
CVE-2008-1234	N/A	N/A	X
CVE-2008-2803	X	N/A	N/A
CVE-2008-2806	X	X	N/A
CVE-2008-4060	N/A	N/A	X
CVE-2008-4062	N/A	X	N/A
CVE-2008-5022	N/A	N/A	X
CVE-2008-5052	X	N/A	N/A
CVE-2008-5506	N/A	N/A	X
CVE-2009-1302	N/A	X	X
CVE-2009-1392	X	N/A	N/A
CVE-2009-1833	N/A	N/A	X
CVE-2009-3983	N/A	N/A	X
CVE-2010-0159	N/A	N/A	X
CVE-2010-0161	X	N/A	X
CVE-2010-0167	X	X	N/A
CVE-2010-0173	N/A	X	N/A
CVE-2010-0179	X	N/A	N/A
CVE-2010-1585	X	N/A	N/A
CVE-2010-2767	X	N/A	N/A
CVE-2010-3181	N/A	N/A	X
CVE-2011-0053	N/A	X	N/A
CVE-2011-0081	N/A	X	N/A
CVE-2011-2362	N/A	N/A	X
CVE-2011-2372	N/A	N/A	X
CVE-2011-2985	N/A	N/A	X
CVE-2011-2995	N/A	X	X
CVE-2011-2997	N/A	X	N/A
CVE-2011-3001	X	N/A	X
CVE-2011-3647	X	N/A	N/A
CVE-2011-3660	N/A	X	X
CVE-2011-3664	X	N/A	N/A
CVE-2012-0446	X	N/A	N/A
CVE-2012-0461	N/A	X	X
CVE-2012-0467	N/A	X	X
CVE-2012-1956	X	N/A	N/A
CVE-2012-3960	X	N/A	N/A
CVE-2012-3975	X	N/A	N/A
CVE-2012-3994	X	N/A	N/A
CVE-2012-4194	X	N/A	N/A
CVE-2012-4195	X	N/A	N/A
CVE-2012-4201	X	N/A	N/A
CVE-2012-4205	X	N/A	N/A
CVE-2012-4209	X	N/A	N/A
CVE-2012-5354	X	N/A	N/A

CVE-2013-0747	X	X	X
CVE-2013-0756	N/A	N/A	X
CVE-2013-0758	X	X	X
CVE-2013-0760	N/A	N/A	X
CVE-2013-0779	N/A	N/A	X
CVE-2013-0784	N/A	X	N/A
CVE-2013-0791	X	N/A	N/A
CVE-2013-0801	N/A	X	X
CVE-2013-1679	X	X	X
CVE-2013-1713	X	X	X
CVE-2013-1717	N/A	X	X
CVE-2013-1718	N/A	N/A	X
CVE-2013-1719	N/A	N/A	X
CVE-2014-1509	X	N/A	N/A
CVE-2014-1513	N/A	N/A	X
CVE-2014-1514	N/A	N/A	X
CVE-2014-1518	N/A	N/A	X
CVE-2014-1539	N/A	X	N/A
CVE-2014-1595	N/A	N/A	X
CVE-2015-0813	X	N/A	N/A
CVE-2015-2724	N/A	X	X
CVE-2015-2725	N/A	X	X
CVE-2016-1966	X	X	X

## WordPress CVEs

CVE ID	Keword-based	Component-based	File-based
CVE-2005-4463	X	N/A	N/A
CVE-2006-5705	X	N/A	N/A
CVE-2007-5800	X	N/A	N/A
CVE-2007-6677	X	N/A	N/A
CVE-2008-0198	X	N/A	N/A
CVE-2008-0491	X	N/A	N/A
CVE-2008-0615	X	N/A	N/A
CVE-2008-0616	X	N/A	N/A
CVE-2008-0617	X	N/A	N/A
CVE-2008-0618	X	N/A	N/A
CVE-2008-1982	X	N/A	N/A
CVE-2008-4625	X	N/A	N/A
CVE-2008-4732	X	N/A	N/A
CVE-2008-4733	X	N/A	N/A
CVE-2008-4734	X	N/A	N/A
CVE-2008-5695	X	N/A	N/A

CVE-2008-5752	X	N/A	N/A
CVE-2008-6811	X	N/A	N/A
CVE-2008-7175	X	N/A	N/A
CVE-2009-0968	X	N/A	N/A
CVE-2009-2122	X	N/A	N/A
CVE-2009-2143	X	N/A	N/A
CVE-2009-2144	X	N/A	N/A
CVE-2009-2334	X	N/A	N/A
CVE-2009-2383	X	N/A	N/A
CVE-2009-2396	X	N/A	N/A
CVE-2009-2852	X	N/A	N/A
CVE-2009-3703	X	N/A	N/A
CVE-2009-4168	X	N/A	N/A
CVE-2009-4169	X	N/A	N/A
CVE-2009-4170	X	N/A	N/A
CVE-2009-4424	X	N/A	N/A
CVE-2009-4672	X	N/A	N/A
CVE-2009-4748	X	N/A	N/A
CVE-2010-0673	X	N/A	N/A
CVE-2010-1186	X	N/A	N/A
CVE-2010-2924	X	N/A	N/A
CVE-2010-3977	X	N/A	N/A
CVE-2010-4277	X	N/A	N/A
CVE-2010-4402	X	N/A	N/A
CVE-2010-4403	X	N/A	N/A
CVE-2010-4518	X	N/A	N/A
CVE-2010-4630	X	N/A	N/A
CVE-2010-4637	X	N/A	N/A
CVE-2010-4747	X	N/A	N/A
CVE-2010-4779	X	N/A	N/A
CVE-2010-4825	X	N/A	N/A
CVE-2010-4839	X	N/A	N/A
CVE-2010-4875	X	N/A	N/A
CVE-2010-5295	X	N/A	X
CVE-2011-0641	X	N/A	N/A
CVE-2011-0759	X	N/A	N/A
CVE-2011-0760	X	N/A	N/A
CVE-2011-1047	X	N/A	N/A
CVE-2011-3841	X	N/A	N/A
CVE-2011-3981	X	N/A	N/A
CVE-2011-4342	X	N/A	N/A
CVE-2011-4562	X	N/A	N/A
CVE-2011-4568	X	N/A	N/A
CVE-2011-4618	X	N/A	N/A

CVE-2011-4646	X	N/A	N/A
CVE-2011-4669	X	N/A	N/A
CVE-2011-4671	X	N/A	N/A
CVE-2011-4673	X	N/A	N/A
CVE-2011-4803	X	N/A	N/A
CVE-2011-4926	X	N/A	N/A
CVE-2011-5051	X	N/A	N/A
CVE-2011-5082	X	N/A	N/A
CVE-2011-5104	X	N/A	N/A
CVE-2011-5106	X	N/A	N/A
CVE-2011-5107	X	N/A	N/A
CVE-2011-5128	X	N/A	N/A
CVE-2011-5179	X	N/A	N/A
CVE-2011-5180	X	N/A	N/A
CVE-2011-5181	X	N/A	N/A
CVE-2011-5182	X	N/A	N/A
CVE-2011-5191	X	N/A	N/A
CVE-2011-5192	X	N/A	N/A
CVE-2011-5193	X	N/A	N/A
CVE-2011-5194	X	N/A	N/A
CVE-2011-5207	X	N/A	N/A
CVE-2011-5208	X	N/A	N/A
CVE-2011-5216	X	N/A	N/A
CVE-2011-5224	X	N/A	N/A
CVE-2011-5225	X	N/A	N/A
CVE-2011-5226	X	N/A	N/A
CVE-2011-5254	X	N/A	N/A
CVE-2011-5264	X	N/A	N/A
CVE-2011-5265	X	N/A	N/A
CVE-2012-0898	X	N/A	N/A
CVE-2012-0934	X	N/A	N/A
CVE-2012-1010	X	N/A	N/A
CVE-2012-1011	X	N/A	N/A
CVE-2012-1067	X	N/A	N/A
CVE-2012-1068	X	N/A	N/A
CVE-2012-1125	X	N/A	N/A
CVE-2012-1205	X	N/A	N/A
CVE-2012-1785	X	N/A	N/A
CVE-2012-1786	X	N/A	N/A
CVE-2012-1835	X	N/A	N/A
CVE-2012-2109	X	N/A	N/A
CVE-2012-2371	X	N/A	N/A
CVE-2012-2402	X	N/A	X
CVE-2012-2759	X	N/A	N/A
CVE-2012-2912	X	N/A	N/A
CVE-2012-2913	X	N/A	N/A
CVE-2012-2916	X	N/A	N/A
CVE-2012-2917	X	N/A	N/A
CVE-2012-2920	X	N/A	N/A

CVE-2012-3574	X	N/A	N/A
CVE-2012-3575	X	N/A	N/A
CVE-2012-3576	X	N/A	N/A
CVE-2012-3577	X	N/A	N/A
CVE-2012-3578	X	N/A	N/A
CVE-2012-3588	X	N/A	N/A
CVE-2012-3814	X	N/A	N/A
CVE-2012-4033	X	N/A	N/A
CVE-2012-4242	X	N/A	N/A
CVE-2012-4263	X	N/A	N/A
CVE-2012-4264	X	N/A	N/A
CVE-2012-4268	X	N/A	N/A
CVE-2012-4271	X	N/A	N/A
CVE-2012-4272	X	N/A	N/A
CVE-2012-4273	X	N/A	N/A
CVE-2012-4283	X	N/A	N/A
CVE-2012-4327	X	N/A	N/A
CVE-2012-4332	X	N/A	N/A
CVE-2012-4422	X	N/A	N/A
CVE-2012-4874	X	N/A	N/A
CVE-2012-4915	X	N/A	N/A
CVE-2012-4920	X	N/A	N/A
CVE-2012-5177	X	N/A	N/A
CVE-2012-5178	X	N/A	N/A
CVE-2012-5229	X	N/A	N/A
CVE-2012-5310	X	N/A	N/A
CVE-2012-5318	X	N/A	N/A
CVE-2012-5325	X	N/A	N/A
CVE-2012-5327	X	N/A	N/A
CVE-2012-5328	X	N/A	N/A
CVE-2012-5349	X	N/A	N/A
CVE-2012-5350	X	N/A	N/A
CVE-2012-5387	X	N/A	N/A
CVE-2012-5388	X	N/A	N/A
CVE-2012-5469	X	N/A	N/A
CVE-2012-5856	X	N/A	N/A
CVE-2012-6312	X	N/A	N/A
CVE-2012-6313	X	N/A	N/A
CVE-2012-6499	X	N/A	N/A
CVE-2012-6506	X	N/A	N/A
CVE-2012-6527	X	N/A	N/A
CVE-2013-0721	X	N/A	N/A
CVE-2013-0731	X	N/A	N/A
CVE-2013-0734	X	N/A	N/A
CVE-2013-0735	X	N/A	N/A
CVE-2013-0736	X	N/A	N/A
CVE-2013-1409	X	N/A	N/A
CVE-2013-1464	X	N/A	N/A
CVE-2013-1949	X	N/A	N/A

CVE-2013-2201	X	N/A	N/A
CVE-2013-2204	X	N/A	N/A
CVE-2013-2501	X	N/A	N/A
CVE-2013-2640	X	N/A	N/A
CVE-2013-2696	X	N/A	N/A
CVE-2013-2697	X	N/A	N/A
CVE-2013-2702	X	N/A	N/A
CVE-2013-2703	X	N/A	N/A
CVE-2013-2704	X	N/A	N/A
CVE-2013-2706	X	N/A	N/A
CVE-2013-2707	X	N/A	N/A
CVE-2013-2709	X	N/A	N/A
CVE-2013-2741	X	N/A	N/A
CVE-2013-2742	X	N/A	N/A
CVE-2013-2743	X	N/A	N/A
CVE-2013-2744	X	N/A	N/A
CVE-2013-3253	X	N/A	N/A
CVE-2013-3254	X	N/A	N/A
CVE-2013-3256	X	N/A	N/A
CVE-2013-3261	X	N/A	N/A
CVE-2013-3262	X	N/A	N/A
CVE-2013-3479	X	N/A	N/A
CVE-2013-3487	X	N/A	N/A
CVE-2013-3491	X	N/A	N/A
CVE-2013-3526	X	N/A	N/A
CVE-2013-3529	X	N/A	N/A
CVE-2013-3530	X	N/A	N/A
CVE-2013-3532	X	N/A	N/A
CVE-2013-3720	X	N/A	N/A
CVE-2013-4117	X	N/A	N/A
CVE-2013-4625	X	N/A	N/A
CVE-2013-4626	X	N/A	N/A
CVE-2013-4944	X	N/A	N/A
CVE-2013-4954	X	N/A	N/A
CVE-2013-5098	X	N/A	N/A
CVE-2013-5672	X	N/A	N/A
CVE-2013-5673	X	N/A	N/A
CVE-2013-5714	X	N/A	N/A
CVE-2013-5917	X	N/A	N/A
CVE-2013-5918	X	N/A	N/A
CVE-2013-5961	X	N/A	N/A
CVE-2013-5963	X	N/A	N/A
CVE-2013-6010	X	N/A	N/A
CVE-2013-6991	X	N/A	N/A
CVE-2013-6992	X	N/A	N/A
CVE-2013-6993	X	N/A	N/A
CVE-2013-7240	X	N/A	N/A
CVE-2013-7276	X	N/A	N/A
CVE-2013-7279	X	N/A	N/A

CVE-2014-1232	X	N/A	N/A
CVE-2014-1888	X	N/A	N/A
CVE-2014-1907	X	N/A	N/A
CVE-2014-2315	X	N/A	N/A
CVE-2014-2316	X	N/A	N/A
CVE-2014-3210	X	N/A	N/A
CVE-2014-3841	X	N/A	N/A
CVE-2014-3843	X	N/A	N/A
CVE-2014-3844	X	N/A	N/A
CVE-2014-3845	X	N/A	N/A
CVE-2014-4529	X	N/A	N/A
CVE-2014-4534	X	N/A	N/A
CVE-2014-4600	X	N/A	N/A
CVE-2014-4603	X	N/A	N/A

# Chromium

## CVE-2016-1650

### Context

The flaw occurs in an API used by extensions for doing a page capture

### Problem

There is a race condition when a failure occurs in the PageCaptureSaveAsMHTMLFunction extension function (pageCapture.saveAsMHTML). There are a few different ways the use-after-free can occur, but suppose we have the following background extension script: chrome.pageCapture.saveAsMHTML({"tabId": 1337}, function(results) {}); When this function's RunAsync() is called, a single AddRef() is called to add an additional reference to the function. This is "balanced" with a Release() in ReturnFailure(), and in OnMessageReceived(). The problem is that it's possible for both Release()s to be called causing a race condition and a uaf crash.

### Solution

Remove extra Release() in pageCapture extension function implementation.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=597518>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=401364>

### Commit URL

- <https://codereview.chromium.org/1761303003/>

## CVE-2016-1640

### Context

The Web Store inline-installer implementation in the Extensions UI in Google Chrome before 49.0.2623.75 does not block installations upon deletion of an installation frame, which makes it easier for remote attackers to trick a user into believing that an installation request originated from the user's next navigation target via a crafted web site.

### Problem

An installation can only trigger an extension install that is hosted in the same origin of the site who triggered the install. This vulnerability makes it possible to display an inline extension installation dialog on a different origin that initiated the install. Thus tricking the user into installing an Extension as if it was from that origin. As the dialog doesn't show the origin, it gives even more credibility to the attack.

### Solution

Don't allow inline install if frame is deleted before user accepts. If the frame that called the chrome.webstore.install method to begin an inline install gets deleted before the user accepts from the dialog, we don't want the install to continue because a navigation could make it look like the install request was coming from some unrelated site. One downside of this approach is that the dialog stays around even after the frame is deleted, and hitting either accept or cancel buttons both just cancel the install. It would be better if the dialog is automatically cancelled, but doing that would involve a lot more refactoring. The approach in this CL was easier and is probably worth getting out, and we can improve on it in the future.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=550047>

### Commit URL

- <https://codereview.chromium.org/1496033003>
- <https://codereview.chromium.org/1554233005>

## CVE-2016-1638

### Context

Restrictions can be bypassed, which allows remote attackers to bypass intended access restrictions via a crafted platform app.

### Problem

Chrome Version: 48.0.2564.103 (stable, and earlier) and 50.0.2633.0 (HEAD) Some web platform APIs are disabled in Chrome apps for security reasons ([https://developer.chrome.com/apps/app\\_deprecated](https://developer.chrome.com/apps/app_deprecated)). This is implemented in platform\_app.js [1]. These restrictions can be bypassed: (I) The restriction of document.open/write/writeln/close is implemented by shadowing HTMLDocument.prototype.write, but Document.prototype.write should be shadowed instead. So, either of the following two ways allows the use of the restricted API: delete HTMLDocument.prototype.write; Document.prototype.write.call(document); (II) window.onbeforeunload is shadowed by Object.defineProperty with configurable:true. This allows the property descriptor to be removed via the delete operator: delete window.onbeforeunload; // Remove restriction window.onbeforeunload = function() { return 'This should not be visible!'; }; PoC for I: See issue 585268 (document.write/close was used for that exploit). PoC for II: 1. Download manifest.json and background.js 2. Load the app (either via chrome://extensions, or by uploading it to the Chrome Web Store and installing it). 3. The app uses the above trick, and then calls location.reload() to show a PoC. Expected result: "window.onbeforeunload is not available in packaged apps." error in console. Actual result : Upon unload, a dialog shows up.

### Solution

It's easy enough to patch these particular issues - disable the methods on Document instead of HTMLDocument, don't do strict comparisons for onunload and related, remove the configurable, etc. The underlying problem though is that we're trying to mangle things in JS that really should fundamentally be guaranteed at a lower level (probably somewhere in blink). Unfortunately, I don't know the best way to begin going about that (or if it's even necessarily something we really want to do), and don't personally have time to implement it at the moment. If anyone knows a way that this is already done in blink (or content/, or v8), lemme know - in the meantime, I'll go ahead and make these fixes to at least harden our security a little bit.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=585282>

### Commit URL

- <https://codereview.chromium.org/1744623002>

## CVE-2016-1635

### Context

extensions::LoadWatcher::CallbackAndDie is called when DidCreateDocumentElement is triggered. CallbackAndDie calls a user-defined JavaScript function and then deletes the LoadWatcher instance. However, JavaScript code can easily replace the document (e.g. via document.close/write) and DidCreateDocumentElement is triggered also whenever a document is created/replaced.

### Problem

Malicious Chrome apps can cause CallbackAndDie to be called re-entrantly when the callback of chrome.apps.window.create replaces the document of the new app window, which results in a use-after-free. This results in a crash of the Web browser.

### Solution

Avoid re-entrant calls by using PostTask through observer notifications that the method has been called once and has not finished executing.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=585268>

### Commit URL

- <https://codereview.chromium.org/1684953002>

## CVE-2016-1622

### Context

The Object.defineProperty() method defines a new property directly on an object, or modifies an existing property on an object, and returns the object. It was being used as an attack vector.

### Problem

Malicious parties can change the content of an extension through its code being able to be accessed through Object.defineProperty method. This allows third parties to change the behavior of the extension through crafted Javascript code.

This results in a Same-Origin Policy bypass.

### Solution

Don't allow built-in extensions code to be overridden.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=546677>

### Commit URL

- <https://codereview.chromium.org/1417513003>

## CVE-2015-6779

### Context

PDFium, as used in Google Chrome before 47.0.2526.73, does not properly restrict use of chrome: URLs, which allows remote attackers to bypass intended scheme restrictions via a crafted PDF document, as demonstrated by a document with a link to a chrome://settings URL.

### Problem

A hyperlink inside a pdf file shown by the chrome pdf-viewer can link to a chrome:// url and can be opened as a new tab. As this is prohibited in html (it will open about:blank), it also shouldn't be possible in a pdf-file. PDF viewer allows navigation to file:// URLs, whereas it does not for webpages.

### Solution

a mechanism for more granular link URL permissions (filtering on scheme/host). This fixes the bug that allowed PDFs to have working links to any "chrome://" URLs

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=528505>

### Commit URL

- <https://codereview.chromium.org/1362433002>

## CVE-2015-6772

### Context

Security: Universal XSS using plugin objects Google chromium allows that elements are attached/detached at runtime using javascript. Each attached document in iframes is checked against the Same-Origin Policy

### Problem

This is a regression from issue 524120. Now that widget updates are deferred until after the frame is detached from the document (and beyond the lifetime of ScriptForbiddenScope, too), it is possible to attach another document to the frame before a new document is installed. The attached document can then be used to bypass the same-origin policy. "So the root cause of this issue is that running nested message loops that invoke script in Document::detach() generally results in broken invariants. The original patch tries to change the timing of running deferred widget updates to the message loop, to avoid re-entrancy. However, that hit a lot of crashes and didn't look like something that would be easy to merge to M47. Another patch:https://codereview.chromium.org/1444183003 works but it turns out that it can leave a dangling Document/FrameView. The invariant being violated here is that Frame has no FrameView at the end of Document::detach().

### Solution

"Note that the change looks large, but it's really just moving FrameNavigationDisabler from NavigationScheduler into LocalFrame. The core change in the patch is just adding one line to Document::detach to disable navigations: FrameNavigationDisabler navigationDisabler("m\_frame"); Which is really low risk because prior to r350972, these sorts of navigations couldn't be triggered anyway."

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=546545>

### Commit URL

- <https://codereview.chromium.org/1444183003/>

## CVE-2015-1302

### Context

Security: Cross-site read access to PDF files. Pdf Data leakage across cross-origin.

### Problem

The out-of-process viewer exposes an API when its MIME-type is set to application/x-google-chrome-pdf, presumably to support the print preview. Among the supported API is a method to select all text and get the contents of the selection. This allows any web page to read the contents of a PDF file from any source.

I have attached a proof of concept.

1. Open the page.
2. Input the URL of a PDF file (I've used the Bitcoin paper as an example).
3. Click on the "Show content" button.
4. The contents of the PDF will be displayed in the PDF.

This can be fully automated, websites could scan for popular URLs and automatically read the contents of a PDF. The only defence for users is to disable plugin loading by default. There are three settings, "Run all plugin content", "Detect and run important plugin content" and "Let me choose when to run plugin content". Only the last option protects users from this exploit.

### Solution

insert an iframe (containing a page from ChromeVox's origin) that directly communicates with the PDF component extension, via a MessagePort. The sender and receiver have to mutually authenticate each other, this can be done by communicating a random value over another channel (e.g. extension message passing API). - Run ChromeVox in the component extension, and directly communicate between the component extension and ChromeVox.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=520422>

### Commit URL

- <https://codereview.chromium.org/1316803003>

## CVE-2015-1298

### Context

The chrome.runtime is exposed for app developers to access some information about the underlying runtime environment, as stated in the documentation: "Use the chrome.runtime API to retrieve the background page, return details about the manifest, and listen for and respond to events in the app or extension lifecycle. You can also use this API to convert the relative path of URLs to fully-qualified URLs." Source: <https://developer.chrome.com/apps/runtime#method-setUninstallURL>

### Problem

chrome.runtime.setUninstallURL only checks whether the given parameter is a syntactically valid URL, but it does not enforce the blacklist of disallowed URLs. This allows extensions and apps (without requiring any install permissions) to open any URL, including special chrome:// URLs. In the worst case, this bug could be used to exploit a memory bug in the browser process (e.g. UAF in a browser thread upon shutdown).

### Solution

To restrict chrome.runtime.setUninstallURL to http(s). Disallow URLs other than http(s) in chrome.runtime.setUninstallURL. And allow empty URLs to be set to clear the uninstallation URL. Added an optional callback, to know when setting the URL finished (or failed).

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=518827>

### Commit URL

- <https://codereview.chromium.org/1282263002/>

## CVE-2015-1297

### Context

The WebRequest API implementation in extensions/browser/api/web\_request/web\_request\_api.cc in Google Chrome before 45.0.2454.85 does not properly consider a request's source before accepting the request, which allows remote attackers to bypass intended access restrictions via a crafted (1) app or (2) extension.

### Problem

webRequest API allows extensions to intercept and redirect requests from the browser. That includes requests from other extensions. However, it also allows to intercept XMLHttpRequest requests from Chrome Apps, which is quite possibly unintended. Chrome Apps are supposed to be as much independent from the browser as possible.

### Solution

Hide requests in an extension from other extensions

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=510802>

### Commit URL

- <https://codereview.chromium.org/1267183003/>

## CVE-2015-1226

### Context

Extensions API: The DebuggerFunction::InitAgentHost function in browser/extensions/api/debugger/debugger\_api.cc in Google Chrome before 41.0.2272.76 does not properly restrict what URLs are available as debugger targets, which allows remote attackers to bypass intended access restrictions via a crafted extension.

### Problem

Extensions can silently debug (run code) in ANY tab and escape the sandbox. The chrome.debugger extension API can attach to targets at any origin, including URLs such as file://, chrome://, chrome-extension:// and the Chrome Web store. Attaching to privileged targets is usually forbidden when the target is specified by tabId or extensionId. However, it is also possible to attach to a target by targetId, which is not subjected to any validation. This targetId can easily be obtained using the chrome.debugger.getTargets method. Because of these capabilities, anything that can be displayed in a tab is completely compromised when a user installs an extension that exploits this bug.

#### Solution

Validate debuggee.targetId before use in chrome.debugger and refactored the tests to make sure that the debugger is detached upon returning from RunAttachFunction. Previously, if the debugger unexpectedly succeeded in attaching, the method would return (because empty error != some error), causing the attached debugger to not be detached. In short, they added a permission check

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=456841>

#### Commit URL

- <https://codereview.chromium.org/910053002>

## CVE-2014-3172

#### Context

The Debugger extension API in browser/extensions/api/debugger/debugger\_api.cc in Google Chrome before 37.0.2062.94 does not validate a tab's URL before an attach operation, which allows remote attackers to bypass intended access limitations via an extension that uses a restricted URL, as demonstrated by a chrome:// URL.

#### Problem

Any extension can debug any other extension, and be able to maliciously use the data of users. By using the "downloads" permission in conjunction with network\_diag, network\_logging, wpa\_debug, and ff\_debug it should be possible to snoop on a lot of private user data.

#### Solution

Have the Debugger extension api check that it has access to the tab CheckPermissionsData::CanAccessTab() prior to attaching the debugger.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=367567>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=280354&view=revision>

## CVE-2014-3170

#### Context

Extensions/common/url\_pattern.cc in Google Chrome before 37.0.2062.94 does not prevent use of a '\0' character in a host name, which allows remote attackers to spoof the extension permission dialog by relying on truncation after this character.

#### Problem

By inserting a NUL byte in a host permission, extension authors can hide all host permission requests, giving users a false sense of security when they install an extension.

#### Solution

Do not allow NUL characters in the hosts of host permissions.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=390624>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=285492&view=revision>

## CVE-2014-1728

#### Context

out of bounds writes A Pwnium 4 entry achieved a sandbox escape by sending messages from a compromised swapped out renderer to a vulnerable extension. The problem seems to be in TabHelper, which is getting state confused by the swap out. creis' synopsis: TabHelper is not deleting state associated with a swapped out RVH. It should probably be listening to WebContentsObserver::RenderViewHostChanged in addition to RenderViewHostCreated.

#### Problem

The exploit is possible because the attacker's renderer process can send a message from a swapped out RenderFrameHost which makes it up into TabHelper. TabHelper isn't keeping track of who sent the message and assumes it's from WebContents::GetRenderViewHost(), which refers to the current RenderViewHost (legitimately for the extension process) and not the swapped out one (in the attacker's process). Multiple things are wrong here: 1) A message from a swapped out RFH is making it up to TabHelper. Swapped out hosts shouldn't be propagating their IPC messages up to observers. We actually have a check for that in RenderViewHostImpl::OnMessageReceived, where we filter out such IPC messages using CanHandleWhileSwappedOut. We're missing that check in RenderFrameHostImpl, which is how this snuck through. Nasko will fix that. 2) TabHelper doesn't know who sent it the message, since that information is not available in OnMessageReceived. In theory, it would be nice for it not to have to worry about that, since it's easy to miss an access control check. Fixing (1) means we don't have to worry about messages from swapped out RFHs, for example. Unfortunately, the problem still exists with current vs pending RFHs. More concretely, a WebContents can have both a current and a pending RFH at the same time (e.g., one in an attacker's process and one in an extension process). Until the pending RFH actually commits, IPC messages could come up to WebContentsObservers from either one, and the observers just assume that they're hearing from the current RFH, not the pending one. That could lead to the same kind of attack.

#### Solution

More concretely, a WebContents can have both a current and a pending RFH at the same time (e.g., one in an attacker's process and one in an extension process). Until the pending RFH actually commits, IPC messages could come up to WebContentsObservers from either one, and the observers just assume that they're hearing from the current RFH, not the pending one. That could lead to the same kind of attack. I'm not sure if it's possible to hide messages from the pending RFH until it commits, since it may need to initialize state (e.g., RenderFrameCreated) before the commit happens. Queuing the messages up inside WebContents until commit might be possible, but that feels really error prone if it delays acks or other message exchanges. Another option is to expose who sent the IPC message so that the observer can do an access

control check. Exposing "who sent it" could be in the form of RenderFrameHost, routing ID + process ID, SiteInstance, or some kind of security principal. Longer term efforts like Mojo might help with that. In the shorter term, it's less clear how to fix that without exposing concepts like pending RFHs to observers.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=358059>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=350863>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=352982>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=354297>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=351815>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=360298>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=350533>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=350537>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=347262>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=356235>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=356517>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=345820>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=355586>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=353013>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=348319>

#### Commit URL

- <http://src.chromium.org/viewvc/blink?view=rev&revision=167957>

## CVE-2013-2912

#### Context

Heap-use-after-free in ppapi::proxy::PluginResource::NotifyInstanceWasDeleted. A refactoring was suggested but reverted because it broke Docs print preview. A little more printf debugging reveals that the PluginResource destructor sends the destruct message to the host but never exits. It looks like a hang, but there shouldn't be multiple threads for in-process plugins.

#### Problem

A unique situation for in-process plugins. The repro.html file causes a load to start, then a reload, then moves the plugin element when the ready state changes. The instance is torn down while we're in one of the URLLoaderResource dtors, before it has removed itself from the tracker. The resource tracker tries to use the object which is half destroyed. The repro.html forces it into a state it doesn't like, hitting a NOTREACHED which needs to be changed.

#### Solution

Change the PepperInProcessRouter to defer resource destruction messages. This changes the in process "proxy" so it posts tasks to send resource destruction messages instead of calling them directly. This prevents several kinds of re-entrancy into the plugin-side code. In this case, when a URLLoader is released, the plugin can finish before the host cancels the load and potentially deletes the instance.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=276368>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=222614&view=revision>

## CVE-2013-2876

#### Context

Extensions UI- browser/extensions/api/tabs/tabs\_api.cc in Google Chrome before 28.0.1500.71 does not properly enforce restrictions on the capture of screenshots by extensions, which allows remote attackers to obtain sensitive information about the content of a previous page via vectors involving an interstitial page.

#### Problem

Extensions are allowed to screenshot interstitial websites content without having permission to do so, hence being able to steal user's information.

#### Solution

Add check for permission screenshot even in interstitial websites or not allow it by default.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=229504>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=198297&view=revision>

## CVE-2013-2868

#### Context

common/extensions/sync\_helper.cc in Google Chrome before 28.0.1500.71 proceeds with sync operations for NPAPI extensions without checking for a certain plugin permission setting, which might allow remote attackers to trigger unwanted extension changes via unspecified vectors.

#### Problem

Chrome Sync is used to install an extension with NPAPI plugin and execute code. Though extensions with plugins cannot be installed through sync directly, they can be auto-updated, and the new version may contain plugins. chrome/common/extensions/sync\_helper.cc checks PluginsInfo::HasPlugins to determine if an extension can be synced. HasPlugins returns false if there's an empty plugins section. chrome/common/extensions/api/plugins/plugins\_handler.cc parses "plugins" from the manifest. It treats an empty "plugins" section differently from it not being there, though. It also adds the "plugins" permission if there are any plugins; it should be treated as a permissions increase (disabling the extension) if there are new plugins in the new version of the extension.

#### Solution

The fix adds a check for |plugin| permission while syncing NPAPI plugins.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=252034>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=207830&view=revision>

## CVE-2013-2841

#### Context

Use-after-free vulnerability allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of Pepper resources. generic WebKit DOM vs. PPAPI URL loading lifetime issue.

#### Problem

1. PPB\_URLLoader\_Impl(ppb\_url\_loader\_impl.h) is a subclass of ppapi::Resource(ppapi/shared\_impl/resource.h). 2. But for some strange reason destructor of ppapi::Resource is not executed when destructor of PPB\_URLLoader\_Impl is executed. 3. Think that is why this bug happens. Because destructor of ppapi::Resource should be executed to remove PPB\_URLLoader\_Impl instance from ResourceMap live\_resources\_ of ResourceTracker(ppapi/shared\_impl/resource\_tracker.cc). 4. Otherwise PPB\_URLLoader\_Impl instance will remain in ResourceMap live\_resources\_ of ResourceTracker even after being deleted.

#### Solution

Remove Pepper URLLoader from resource tracker early. This protects against double delete if the instance is destroyed as a result of canceling a load.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=227350>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=197686&view=revision>

## CVE-2013-0925

#### Context

Google Chrome before 26.0.1410.43 does not ensure that an extension has the tabs (aka APIPermission::kTab) permission before providing a URL to this extension, which has unspecified impact and remote attack vectors.

#### Problem

The chrome.tabs.onUpdated event is accessible to Chrome extensions even without the "tabs" permission, and leaks the URLs the user navigates to in the changeInfo.url argument to the event callback.

#### Solution

Do not pass URLs in onUpdated events to extensions unless they have the "tabs" permission.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=168442>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=176406&view=revision>

## CVE-2013-0924

#### Context

When you install an extension, there are warnings about host permissions. However, by design there aren't any for file: permissions - these are handled via a checkbox on the extension settings page. The same goes for the permissions API.

#### Problem

The API implementation doesn't respect the checkbox value on the extensions settings page, so silently allows extensions to obtain file level permissions.

#### Solution

The API implementation should check for the checkbox values by users in the extension settings page that regulate file: permissions.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=169632>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=176853&view=revision>

## CVE-2013-0910

#### Context

Google Chrome before 25.0.1364.152 does not properly manage the interaction between the browser process and renderer processes during authorization of the loading of a plug-in, which makes it easier for remote attackers to bypass intended access restrictions via vectors involving a blocked plug-in.

#### Problem

A compromised renderer can load banned plug. The renderer has the capability to block or unblock plug-in it, but having the decision of block/unblocking a plug-in in the renderer is weak: renderer interacts with content from the Web (untrusted) and may be compromised.

Therefore, a stronger decision is to have the checks of blocks/unblocked plug-ins in the browser-side.

- Allegedly, Java is installed on 66% of computers (largely independent of browser).
- A Java installation is frequently out of date; we block this situation.
- Even when up-to-date, Java is a security nightmare -- it's currently the largest source of severe 0-day attacks in the browser ecosystem. Because of this, we block even an up-to-date Java.

So, interestingly, now think about a compromised renderer. A compromised renderer gets to load any plug-in it pleases. This is largely because the decision to block a plug-in or not lives in the renderer -- and this, in turn, is necessitated by the click-to-play.

However, in the event that the browser determines that the status of a plug-in is "blocked" for whatever reason, we can refuse to load the plug-in at the browser side. This is only slightly complicated by the need to handle browser-mediated user authorizations (infobars, right-click menu and page action icon). So we can become secure against compromised renderers. For example, a compromised renderer now cannot load the Java plug-in by default, unless the user has authorized a site to use Java and the attacker knows what that site is. A majority of users have Java installed yet never use Java. So we can protect those users.

#### Solution

Only permit plug-in loads in the browser if the plug-in isn't blocked or the user has authorized it with a browser-mediated interaction. For example, a compromised renderer now cannot load the Java plug-in by default, unless the user has authorized a site to use Java and the attacker knows what that site is. A majority of users have Java installed yet never use Java. So we can protect those users.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=172573>
- <https://src.chromium.org/viewvc/chrome?view=rev&revision=180103>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=183685&view=revision>

## CVE-2013-0896

#### Context

Plug-in execution. BrowserPluginGuest blindly trusts the size of shared memory regions leading to overflow.

#### Problem

BrowserPluginGuest trusts the shared memory region sizes passed in messages from renderers. When the browser attaches to these regions it does not sanity check the region sizes and can be made to write beyond the end of the mapped region.

#### Solution

Browser Plugin: Simplified BrowserPlugin Damage Buffer  
1. Less platform-specific code.  
2. Use base::SharedMemory instead of TransportDIB.  
3. Use scoped\_ptr to simplify cleanup logic.  
4. More validity checks

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=166708>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=174332&view=revision>

## CVE-2013-0831

#### Context

Extensions > Loading Resources (Directory Path Traversal)

Directory traversal vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to have an unspecified impact by leveraging access to an extension process.

#### Problem

I "found" this via code inspection while looking at an unrelated bug, checking for places where folks might have existing code I could borrow to prevent directory traversal escapes. Consider extension\_resource.cc:66: for (std::vector::const\_iterator i = components.begin(); i != components.end(); i++) { if ("i == FilePath::kParentDirectory) { depth--; } else { depth++; } if (depth < 0) { return FilePath(); } } This logic fails to account for "/" in path names, e.g. given something like ../../ we will be up two levels but will compute depth == 0.

#### Solution

Added a check to enforce that it does not escape the directory

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=161836>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=169949&view=revision>

## CVE-2012-5126

#### Context

Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of plug-in placeholders.

#### Problem

plug-in is being removed from the DOM while we're initializing it

#### Solution

Set the new plug-in on the container before initializing it. Once the plug in is removed , destroy the old plug in

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=156366>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=163802&view=revision>

## CVE-2012-5125

### Context

Extensions > Deallocator

Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.

### Problem

A Use-After-Free that crashes the browser after the extensions is closed. 0. Get a Chrome instrumented with ASan (the one at goto/chrome-asan is a bit stale, but fine). The bug is also reproducible with the ToT Chrome) 1. Install the "Screen Capture by Google" extension (ID: cpngackimfmofbokmjnljamhdncnmpmg) 2. Open any webpage, click on the Screen Capture icon and select "Capture Whole Page" 3. In the Screen Capture window, click the "Close" button.

### Solution

Do not access |this| after this point. Run() ended up closing the tab that owns us. Check that the object is still available before calling it.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=156051>

### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=162556&view=revision>

## CVE-2012-2881

### Context

It is possible to cause webkit to fire a readyystatechange event when pdf object is removed by removing the pdf object on DOMContentLoaded event. Then it is possible to append the removed pdf object back to document which causes a use after free later. Steps ===== 1. Download and host test3.html on local web server. 2. Open test3.html on chrome. 3. Page will display an alert box. Press escape to dismiss alert box or click ok button of alert box. 4. Page will display an alert box again. Press escape to dismiss alert box or click ok button of alert box. 5. Page will display an alert box again for third time. Press escape to dismiss alert box or click ok button of alert box. Chrome will display sad tab due to heap use after free.

### Problem

It is possible to cause webkit to fire a readyystatechange event when pdf object is removed by removing the pdf object on DOMContentLoaded event. Then it is possible to append the removed pdf object back to document which causes a use after free later.

Steps

=====

1. Download and host test3.html on local web server.
2. Open test3.html on chrome.
3. Page will display an alert box.  
Press escape to dismiss alert box or click ok button of alert box.
4. Page will display an alert box again.  
Press escape to dismiss alert box or click ok button of alert box.
5. Page will display an alert box again for third time.  
Press escape to dismiss alert box or click ok button of alert box.  
Chrome will display sad tab due to heap use after free.

Analysis of this issue

=====

1. Web page has embed tag which embeds a pdf file.
2. This embed element is removed on DOMContentLoaded event of document.
3. This causes a readyystatechange event to fire prematurely.
4. Then on readyystatechange event removed embed element is attached to the document again. This is the cause of use after free.

### Solution

ASSERT(!eventDispatchForbidden()) fires when removed plugin re-inserted as part of readyStateChange. Removing a plugin causes a detach which can cancel the last remaining load on a page, resulting in a readyStateChange event during a time when things are inconsistent. Defer the detach which triggers this chain of events until after the node is fully removed from the document's elementsByld map.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=139814>

### Commit URL

- <http://trac.webkit.org/changeset/128524>

## CVE-2012-2880

### Context

race condition with windowless plugin buffers

### Problem

WebPluginProxy::CreateDIBAndCanvasFromHandle() calls scoped\_ptr::reset(). This is deleting a SkCanvas subclass which apparently has a pending paint. Comments in CreateDIB...() suggest this could happen in a chain of multiple resizes. There's a Mac-only special case in Paint() using weak pointers to handle contexts changing during painting. If non-Mac code could change the canvas being used during delegate\_->Paint(), we'd be restoring stage on the wrong canvas.

### Solution

Fix race condition with windowless plugin buffers. The problem, which is already fixed for Mac, is that the buffers can be deleted during a paint because of a resize during an NPN\_Evaluate call. So keep a local reference.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=139462>

### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=151734&view=revision>

## CVE-2012-2878

### Context

Heap-use-after-free in WebKit::WebElement::document  
 m\_pluginWidget member of FrameLoaderClientImpl is keeping the widget alive past the destruction of the document. This keeps the instance registered so that a delayed GetWindowObject is still processed, rather than just erroring upon enter.

### Problem

The plugininstance has a raw ptr to a webplugincontentsimpl which has a raw ptr to an HTMLPluginElement from the document which no longer exists. Now, the m\_pluginWidget is just about to be cleared by FrameLoaderClientImpl::redirectDataToPlugin (called from PluginDocumentParser::appendBytes), but before that can happen, layout causes the plugin to be created, which processes a sync message, which can catch the delayed GetWindowObject in its nested message loop.

### Solution

Check if pluginWidget object is alive

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=137852>

### Commit URL

- <http://trac.webkit.org/changeset/125500>

## CVE-2012-2877

### Context

Extensions > Sandbox > Process Isolation > Shutdown Chrome extensions bug cause crash in all Chrome processes

### Problem

Chrome extensions bug cause crash in all Chrome processes This crash its most likely a security-related issue, as it is most likely caused by jumping to an illegal address (SEGFAULT). You can see in the example (attached) chrome crash after: xhr.open("GET", "http://api.duckduckgo.com/?q=" + search\_value + "&format=json", true); WinDbg crashes because the active\_dialog of AppModalDialogQueue is non-NULL but garbage. There is a javascript alert open when the popup is dismissed, and the alert dialog is deleted just before the popup is deleted. The root cause is basically in the order the objects destructed: "What's happening is that ExtensionPopup is closing itself directly when it loses focus. This seems to close the alert dialog as well (maybe because it is in the view hierarchy?). The AppModalDialog is deleted as the widget's delegate. The ExtensionHost still isn't deleted in all this time, and won't be deleted until the ExtensionPopup is deleted. The dialog is cancelled from within ~ExtensionHost, and that's where the boom happens."

### Solution

Change the order of the objects destruction, and checks that it is not trying to destroy an already destroyed object

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=137707>

### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=152716&view=revision>

## CVE-2012-2816

### Context

Windows does not properly isolate sandboxed processes, which might allow remote attackers to cause a denial of service (process interference) via unspecified vectors.

### Problem

By default, sandboxed processes can open other sandboxed processes and manipulate them. Integrity levels and the restricted group prevent reaching into unsandboxed processes. However, it's possible to start a renderer with privileged IPCs, open the process, and manipulate it directly. You duplicate the renderer's own process handle with DUPLICATE\_SAME\_ACCESS. Then you can do whatever you want to the process (read/write memory, CreateRemoteThread, etc.).

### Solution

This is a trick to keep the GPU out of low-integrity processes. It starts at low-integrity for UIPI to work, then drops below low-integrity after warm-up.

### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=119150>

### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=132477&view=revision>

## CVE-2011-3956

### Context

Extensions > Privileges Enforcement > Sandbox > Origin In the implementation of extensions privileges

The extension implementation in Google Chrome before 17.0.963.46 does not properly handle sandboxed origins, which might allow remote attackers to bypass the Same Origin Policy via a crafted extension.

### Problem

The iframe sandbox requires that the framed content run under the privileges of a unique origin and not the privileges of the document you downloaded from. But this doesn't seem to be true. Create an extension with a tabs permission, and 2 pages. The first say popup.html runs with full privileges and frames test.html in a sandbox. test.html has code to create a new tab, which should fail since test.html is running under a unique origin. But it doesn't. This is a same-origin bypass.

### Solution

Consider the origin when computing extension permissions This patch teaches the extension system to use the document's origin when computing extension permissions. Ideally, we'd use only the document's origin, but because app extents don't cover entire origins, we need to also consider the document's URL.

### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=103630>

#### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=112655>

## CVE-2011-3107

#### Context

Chrome crashing trying to call hasMethod at <http://trac.webkit.org/browser/trunk/Source/WebCore/bindings/v8/V8NPOObject.cpp?rev=113111#L208>  
Google Chrome before 19.0.1084.52 does not properly implement JavaScript bindings for plug-ins, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.

#### Problem

The NPOObject passed the alive check and has a valid (or null) hasProperty function pointer. However, the hasMethod function pointer is non-null and garbage.

#### Solution

Added a check for NPN\_IsAlive in branches/chromium/1132/Source/WebCore/bindings/v8/NPV8Object.cpp and branches/chromium/1132/Source/WebCore/bindings/v8/V8NPOObject.cpp

#### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=124625>

#### Commit URL

- <https://trac.webkit.org/changeset/117012>

## CVE-2011-3080

#### Context

Race condition in the Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168 allows attackers to bypass intended sandbox restrictions via unspecified vectors.

#### Problem

Sandbox IPC length checking race The bug can be exploited to allow for memory read and write inside the broker process and as such can be exploited to gain code execution, inside the broker process, leading to a complete compromise of broker process and the users machine.

#### Solution

Fix race in CrossCallParamsEx::CreateFromBuffer

#### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=121726>

#### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=130505>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=133531>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=133532>

## CVE-2011-3055

#### Context

The browser native UI in Google Chrome before 17.0.963.83 does not require user confirmation before an unpacked extension installation, which allows user-assisted remote attackers to have an unspecified impact via a crafted extension.

#### Problem

"The invariant that must never be breached is: all extension installs, no matter how initiated, and whether they contain NPAPI or not, must be mediated by a browser dialog."

No permission prompt when loading unpacked extension with NPAPI plugin.

As part of the recent PinkiePie Pwnium exploit, it appears that the attacker was able to gain access to the extensions management page and get it to load an unpacked extension with an NPAPI plugin (see also bug 117715) without generating a prompt. Looking at the code in UnpackedInstaller::OnLoaded, it looks like it should generate a prompt in all cases unless the extension is disabled. It's unclear to me from reading the code if re-enabling the extension would still trigger the prompt, but my guess is that it doesn't. I'm not sure if this is what you were getting at, but I found what appear to be some holes. Say we have version 1 of the extension that has no plugin, and version 2 has a plugin (modifying the manifest in the same location).

This triggers a permission warning:

1. Load unpacked (version 1) from directory
2. Edit the manifest to be version 2 and include plugin section
3. Load unpacked (version 2) from directory

This doesn't trigger a permission warning:

1. Load unpacked (version 1) from directory
2. Disable
3. Edit the manifest to be version 2 and include plugin section
4. Load unpacked (version 2) from directory (it's still disabled)
5. Re-enable

Strangely, this also doesn't trigger a permission warning:

1. Load unpacked (version 1) from directory
2. Edit the manifest to be version 2 and include plugin section
3. 'Reload' the extension from chrome://extensions

#### Solution

To show the prompt message in such scenario (<https://src.chromium.org/viewvc/chrome?revision=119135&view=revision>) "Prevent unnecessary prompts when unpacked extensions use chrome.permissions.request. We now record what permissions have been granted to unpacked extensions to make developing against the permissions API simpler. With this change, chrome.permissions.request will generate the same prompts for packed and unpacked extensions. This also fixes an issue where we were not prompting for unpacked extensions with plugins at installation time."

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=117736>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=127868&view=revision>

## CVE-2011-3049

#### Context

Extensions > Permissions > Malicious Extensions > Blacklist file [SIDE NOTE] There is also a side issue: "Also, I just noticed that the blacklist is downloaded over HTTP. That would allow a man-in-the-middle to arbitrarily blacklist extensions. So, I'll file a separate bug on that one." [...] "the blacklist manifest is fetched over https and includes a sha256 hash - when we fetch the blacklist content over http we verify that the content's hash matches that. See ExtensionUpdater::ProcessBlacklist."

#### Problem

webRequest.onBeforeRequest can intercept calls to [http://www.gstatic.com/chrome/extensions/blacklist/l\\_0\\_0\\_0\\_0\\_7.txt](http://www.gstatic.com/chrome/extensions/blacklist/l_0_0_0_0_7.txt). Thus if an extension went rogue, Google could add the extension to the blacklist but the extension could prevent Chrome from receiving the blacklist update. To exploit the vulnerability, an extension has to put the following code in its background script: chrome.webRequest.onBeforeRequest.addListener(details) { var block = (details.url.indexOf("blacklist") != -1); console.log(details.url, block); return { cancel: block }; }, {urls: ["http:///\*"], ["blocking"]}; After doing so, you should see [http://www.gstatic.com/chrome/extensions/blacklist/l\\_0\\_0\\_0\\_0\\_7.txt](http://www.gstatic.com/chrome/extensions/blacklist/l_0_0_0_0_7.txt) true appear in the background console logs (which means the blacklist URL was successfully blocked). Basically, the listener above executes BEFORE any Web request is performed. Once the URL is the blacklist it blocks the request, which prevents the update.

#### Solution

Hide downloads of extensions blacklist from web request API. This CL prevents that extensions using the web request API can prevent Chrome from updating its extensions blacklist. To do so, they added a method in the WebRequestAPI class to perform such checks:

```
139 // Returns true if the URL is sensitive and requests to this URL must not be modified/canceled by extensions, e.g.  
because it is targeted to the webstore 140 // to check for updates, extension blacklisting, etc. 142 bool IsSensitiveURL(const  
GURL& url) { 143 bool is_webstore_gallery_url = 144 StartsWithASCII(url.spec()), extension_urls::kGalleryBrowsePrefix, true);  
145 bool is_google_com_chrome_url = 146 EndsWith(url.host(), "google.com", true) && 147 StartsWithASCII(url.path(), "/chrome",  
true); 148 std::string url_without_query = 149 url.spec().substr(0, url.spec().find_first_of('?')); 150 return  
is_webstore_gallery_url || is_google_com_chrome_url || 151 extension_urls::IsWebstoreUpdateUrl(GURL(url_without_query)) || 152  
extension_urls::IsBlacklistUpdateUrl(url); 153 }
```

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=108648>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?view=rev&revision=116902>
- <https://src.chromium.org/viewvc/chrome?view=rev&revision=116258>
- <https://src.chromium.org/viewvc/chrome?view=rev&revision=116960>

## CVE-2011-3047

#### Context

The GPU process in Google Chrome before 17.0.963.79 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) by leveraging an error in the plug-in loading mechanism.

#### Problem

The plugin blocking logic wasn't being run for NaCl in prerendering.

#### Solution

Fixed by moving plugin loading in prerendering after the NaCl checks.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=117620>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=117656>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?view=rev&revision=126245>
- <https://src.chromium.org/viewvc/chrome?view=rev&revision=126718>

## CVE-2011-2853

#### Context

Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.

#### Problem

At first glance it looks like no np plugin object is created or it gets deleted because of the empty swf file. Then the window is closed, and chrome tells the np plugin object to release itself (or releases the object, not sure yet).

Either way, there is no such object, only garbage, leading to random memory access in a method call. I'm not sure if it's flash specific or if any np plugin can have this problem. 1. WebKit can have torn down the window script object before getting around to tearing down the plugin, causing any attempt to release the window script object in NPP\_Destroy to reference freed memory. 2. Chromium has a special-case in WebPluginDelegateProxy::PluginDestroyed(), which avoids trying to release the window script object during teardown, by marking it invalid; the comment states that that is done after NPP\_Destroy so that NPP\_Destroy can script the window, which is clearly nonsense if WebKit has already torn it down. The first crash of the three above arises when, while we are blocked waiting for NPP\_Destroy to complete in the plugin process, the plugin sends us an IPC to release the window script object. The third crash of the three above could be referred to ajwong@, if it is easily reproducible

(I haven't observed it myself). The underlying issue is that it's possible for references to a plugin element to cause it to (briefly) out-live its containing page, so that if it scripts the window object during deletion, it may trample freed memory in the renderer.

#### Solution

Cope gracefully with plugin being destroyed during NPObjec tInvoke or Evaluate. Cause the stub to ignore any further IPC messages, and to tear itself down the next time control returns to the message loop. The NPObjec t will be released only if |release\_npobject| is true. This is used for the window script object stub in the renderer, which is freed with NPN\_DeallocateObject to avoid leaks, and so we must not try to release it. void DeleteSoon(bool release\_npobject);

#### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=91197>

#### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=93456>

## CVE-2011-2789

#### Context

Use after free in Pepper plug-in instantiation

#### Problem

It's the stale instance hanging off the resource in ppapi

#### Solution

Maintain a map of all resources in the resource tracker and clear instance back pointers when needed,

#### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=85808>

#### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=89746>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=90056>

## CVE-2011-2785

#### Context

Extensions > Installer > Parsing manifest files

The extensions implementation in Google Chrome before 13.0.782.107 does not properly validate the URL for the home page, which allows remote attackers to have an unspecified impact via a crafted extension.

#### Problem

Extensions manifest can have a "javascript:" url in the "homepage\_url" field. When a user opens the extensions page and clicks on the title of the extension, the homepage for that extension is opened. In this case, the JavaScript is executed in the context of the extensions page. This allows the extension to install another extension from the local file system. The PoC provided by kuzzcc tries to install a second extension that's packaged inside the first. The second extension can have any extension permissions it wants.

#### Solution

While parsing the manifest files, the solution enforces that extensions do not define homepages with schemes other than valid web extents.

#### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=84402>

#### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=87722>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=89006>

## CVE-2011-2783

#### Context

Extensions > UI > prompt user during install. Chrome does not prompt when you use the interface on chrome://extensions to load an unpacked extension that contains an NPAPI plugin.

#### Problem

Missing browser prompt when installing unpacked NPAPI extensions.

Chrome does not prompt when you use the interface on chrome://extensions to load an unpacked extension that contains an NPAPI plugin. We should add the browser prompt to this case as a defense in depth measure against things like <http://crbug.com/83096>.

It seems like the fear here is that someone will XSS chrome://extensions and be able to cause an arbitrary extension to be installed. This is only possible because (it appears) that javascript on chrome://extensions causes a file picker to be displayed then passes the result to C++, who trusts it. The solution is to have C++ show the file picker and never pass the path through JavaScript, not to have this weird dialog that only addresses one case

#### Solution

Show the install dialog for the initial load of an unpacked extension with plugins. For that, created a new callback method at `chrome/browser/extensions/extension_service.h`:

`382 // Called by the backend when an unpacked extension has been loaded.`

`383 void OnLoadSingleExtension(const Extension* extension);`

Then, added a new class (`SimpleExtensionLoadPrompt`) to implement this feature (in `chrome/browser/extensions/extension_service.cc`).

#### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=83273>

#### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=87738>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=87637>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=88403>

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=87655>

## CVE-2011-2358

### Context

[DESIGN-LEVEL] Extensions > UI > prompt user.  
Google Chrome before 13.0.782.107 does not ensure that extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.

### Problem

Android had a bad security bug where you XSS on their gallery led to install on local machine. We can have the same issue on our store because we have no client UI in that case. We do mitigate this issue today by forcing a user gesture. And we also force the client UI in the case of NPAPI.

There is no client-UI-decision for the web store. The decision was made to have an integrated purchase flow, where you only do one confirmation for both money and security, not two separate dialogs.

This means that an XSS results in an install on local machine.

### Solution

Add a webstore install method that lets us prompt the user before downloading. A while back we decided to minimize friction by showing extension/app permissions inline in the webstore, and let installs done via the private webstore API skip the regular extension installation confirmation that happens after downloading and unpacking the .crx file. We've reconsidered this and are now adding a new private install method that lets us go back to having the client display the confirmation dialog, but do it before downloading the .crx file. The webstore just needs to pass the manifest and icon, and then after downloading the .crx we make sure the unpacked extension's manifest matches what we had prompted with.

### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=75821>

### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=83080>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=88606>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=80536>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86780>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=88204>

## CVE-2011-1819

### Context

Malicious extensions modifying protected chrome: URLs

### Problem

A packaged app/extension can access and modify all chrome: pages, read/write preferences, run chrome.send function, pass arguments directly to c++, without required permissions, without using NPAPI plugin, content script or chrome.tabs.executeScript

### Solution

Added an if condition for checking that non-component extensions can only access chrome://favicon and no other // chrome:// scheme urls. if (url.SchemeIs(chrome::kChromeUIScheme) && url.host() != chrome::kChromeUIFaviconHost && location() != Extension::COMPONENT) return false;

### Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=83010>

### Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86164>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86315>

## CVE-2011-1815

### Context

How Chromium protect itself from malicious extension. It happens on the context of manifest files parsing.

Google Chrome before 12.0.742.91 allows remote attackers to inject script into a tab page via vectors related to extensions.

### Problem

Bypass extensions permission: The "web\_url" attribute on a manifest field should not allow javascript: or chrome: URLs. For example, the two manifest files shown below can be used to bypass extensions permissions: manifest1.json ===== { "name": "test", "description": "test", "version": "1", "app": { "launch": { "web\_url": "javascript:alert('document.domain')" } } } manifest2.json ===== { "name": "test", "description": "test", "version": "1", "app": { "launch": { "web\_url": "chrome://history/" } } } In short, extensions can inject the following code through the "web\_url" parameter: - javascript:alert(document.domain) //chrome://newtab - chrome://appcache-internals/ XSS Preconditions: 1. Need to install an extension. No popups will be shown, since the manifest have nothing except web\_url. 2. Open a new tab and click on the app icon. executes in the context of chrome URLs.

### Solution

Make sure that extensions can launch web urls with web safe schemes only. Developers added an if condition to enforce this.

### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=79862>

### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=82297&view=revision>

## CVE-2011-1813

**Context**

There is a stale frame in UserScriptSlave::InjectScripts.

**Problem**

The problem was that the UserScriptIdleScheduler was relying on the FrameDetached notification from its \_original\_ RenderView, to know when it should delete itself since the frame\_ object was gone. But when the frame gets reparented, the FrameDetached only gets sent to observers of the \_new\_ RenderView.

**Solution**

The fix is to have ExtensionHelper, which is per-RenderView, proxy all these calls to ExtensionHelper, which is per-renderer. ExtensionHelper then keeps the map of WebFrame->UserScriptIdleSchedulers, and notifies them of these events.

**Issue Tracking URL**

- <http://bugs.chromium.org/p/chromium/issues/detail?id=78516>

**Commit URL**

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=80988>

**CVE-2011-1450****Context**

Google Chrome before 11.0.696.57 does not properly present file dialogs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."

**Problem**

When an object is destroyed, its select file dialog is not informed to clear its listener which can call back that destroyed object causing a potential for attacks.

**Solution**

Before an object destruction, make sure that its select dialogs are told that the object is gone so that they don't try to call it back.

**Issue Tracking URL**

- <http://bugs.chromium.org/p/chromium/issues/detail?id=77349>

**Commit URL**

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=79507>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=79761>

**CVE-2011-1435****Context**

Extensions leverage the chrome.tabs.captureVisibleTab to capture images of any using a URL like "file://"

**Problem**

The tabs permission for extensions allows an extension to capture an image of any text file, directory, or image from the user's computer via the captureVisibleTab method. Extensions should not be allowed to open web unsafe urls in tabs. Proof of Concept: 1. Download the attached extension. 2. Update the "file" variable in the popup.html file to point to a local text file on your computer (pick something fun, like your private key file). 3. Install the extension. 4. Open the extension's popup (sorry no icon). This all boils down to using the following: chrome.tabs.create({"url": "file:///home//.ssh/id\_rsa"}); chrome.tabs.captureVisibleTab(null, function(d) { // Do something EVIL with 'd'. });

**Solution**

Implement new restrictions on tab.captureVisibleTab() method. It checks that the tab does have "host" permissions to access files in the user's machines: captureVisibleTab() can access some of the same information as JavaScript running on the page. Ensure the extension has host permissions. if (!GetExtension()->CanExecuteScriptOnPage(tab\_contents->GetURL(), NULL, &error\_) { return false; }

**Issue Tracking URL**

- <http://bugs.chromium.org/p/chromium/issues/detail?id=72523>

**Commit URL**

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86114>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86119>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86117>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86116>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86120>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86121>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86112>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=86101>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=74959>

**CVE-2011-1124****Context**

Use-after-free vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to blocked plug-ins.

**Problem**

1. Install out-dated ice-tea java plugin.
2. Open attached crash.html.  
crash.html contains a applet.  
Chrome will show a info bar saying ice-tea java plugin is out-dated.
3. Move the mouse over java applet (Applet is not loaded at this moment, since plugin is outdated).
4. Wait about 3 seconds. crash.html will refresh itself.  
Once the page is refreshed chrome will display a sad tab.

**Solution**

Restore old title in WebViewPlugin only when loading the plugin.

**Issue Tracking URL**

- <http://bugs.chromium.org/p/chromium/issues/detail?id=72437>

**Commit URL**

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=74435>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=74434>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=74428>

**CVE-2011-1123****Context**

It occurs when the extension has a NPAPI plugin and the extension has not specified whether the NPAPI binary is public (i.e., it omitted the "public" attribute in its manifest file).

**Problem**

Take an extension with a non-public: NPAPI plugin: <https://chrome.google.com/extensions/detail/caehdcpeofiigpdhbabnblempncjj?hl=en> "plugins": [ { "path": "plugins/npSwitchy.dll" }, { "path": "plugins/npSwitchy.so" }, { "path": "plugins/npSwitchy64.so" }, { "path": "plugins/iSwitchy.bundle" } ] Then on any public web page, you can instantiate that plugin. var o = document.createElement("OBJECT"); o.type = "application/x-mhdhejazi-switchy-1.6"; document.body.appendChild(o); o.doSomething(); // replace with something dangerous here It's supposed to be the case that in order for this to work that the extension needed to add "public": "true" to their plugin declaration in the manifest: <http://code.google.com/chrome/extensions/npapi.html>

**Solution**

Private extension NPAPI plugins should not be loaded by public web pages. Fixed by adding a check that Web pages should not be calling the PluginList directly.

**Issue Tracking URL**

- <http://bugs.chromium.org/p/chromium/issues/detail?id=72214>

**Commit URL**

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=74149>

**CVE-2011-0779****Context**

Loading of corrupted extension's configuration files.

Google Chrome before 9.0.597.84 does not properly handle a missing key in an extension, which allows remote attackers to cause a denial of service (application crash) via a crafted extension.

**Problem**

VULNERABILITY DETAILS There is a browser crash when loading a corrupted extension file REPRODUCTION CASE 1. Open the attached crx file 2. Click "continue" when prompted 3. The browser crashes The issue is that the crafted extension has an empty signature, that screws it up a memory allocation made in the code while loading the said extension. See Comment #1: We're bombing out on a zero-length allocation in SandboxedExtensionUnpacker::ValidateSignature due to an empty signature. It's a really easy fix; we just need to add the following to the header validation checks we're already doing: if (header.signature\_size == 0) { ReportFailure("Key length is zero"); return false; }

**Solution**

Added a check on SandboxedExtensionUnpacker::ValidateSignature to check for an empty signature. In such case, an error is returned and the loading of the extension is stopped.

**Issue Tracking URL**

- <http://bugs.chromium.org/p/chromium/issues/detail?id=62791>

**Commit URL**

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=65821>

**CVE-2011-0470****Context**

Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle extensions notification, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.

**Problem**

Steps ----- 1. Go to <https://chrome.google.com/extensions/detail/leaabobiocglbbfepphaknffhebpomn> and install the extension - notification will be seen 2. Go to chrome://extensions and uninstall Notification demo extension 3. Exit browser Root cause: for security information, this is a race condition in window closing that can only happen at shutdown. Specifically, at shutdown the browser stops all renderers and additionally forces all windows to close, then the notification code detects the renderer death and tries to close the window a second time, being unaware of the first.

**Solution**

Changed the logic for capturing "window close" events in order to prevent the race condition. Listen for APP\_TERMINATING in notification ui; close windows earlier in the process before they get clobbered by browser\_shutdown leading to a potential double-close.

**Issue Tracking URL**

- <http://bugs.chromium.org/p/chromium/issues/detail?id=58053>

**Commit URL**

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=67883>

**CVE-2010-4491**

## Context

When opening background.html of a malicious extension

Google Chrome before 8.0.552.215 does not properly restrict privileged extensions, which allows remote attackers to cause a denial of service (memory corruption) via a crafted extension.

## Problem

Caused by an use after free. "Looks like installing an extension can cause a use after free in browser process (sandbox escape)."

## Solution

```
Only call WebInspector_syncDispatch if it's actually a function. The frame might have navigated away from the front-end page (which is still weird).
if (dispatchFunction->IsFunction())
return;
```

## Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=62168>

## Commit URL

- <https://trac.webkit.org/changeset/71533>

## CVE-2010-3417

### Context

When extension asks for permission

Google Chrome before 6.0.472.59 does not prompt the user before granting access to the extension history, which allows attackers to obtain potentially sensitive information via unspecified vectors.

### Problem

Installing an extension with only the "history" permission does not generate a "Can access your history" warning (unlike apps with the "tabs" permission). This seems incorrect -- the history API gives even more direct access to user history than the tabs/windows APIs do. For reference, check out this extension <https://chrome.google.com/extensions/detail/cahejgbffgmlmjgdlibphdjejdhagkp> (not mine) which has the history permission but does not generate an install warning.

### Solution

Issue a warning in the above scenario

## Issue Tracking URL

- <http://bugs.chromium.org/p/chromium/issues/detail?id=54006>

## Commit URL

- <http://src.chromium.org/viewvc/chrome?view=rev&revision=58285>
- <http://src.chromium.org/viewvc/chrome?view=rev&revision=58251>

## CVE-2010-3250

### Context

When Webpages attempt to load resources from extensions.

Unspecified vulnerability in Google Chrome before 6.0.472.53 allows remote attackers to enumerate the set of installed extensions via unknown vectors.

### Problem

Web pages should NOT be able to load resources if there are NO content scripts from that extension on the page. We allow web pages to load resources from extensions as a feature to content scripts. However, if we know that an extension does not have any content scripts on a page, then we should not allow resources to be loaded from that extension. Summary: Refactored extension privilege enumeration and implemented URLPattern comparisons. This will allow checks on per origin extension resource access. Added origin check when loading extension resources.

### Solution

Refactored extension privilege enumeration and implemented URLPattern comparisons. This will allow checks on per origin extension resource access. Added origin check when loading extension resources. Details: 1. Modify Extension::GetEffectiveHostPermissions() to return an ExtensionExtent (chrome/common/extensions/extension\_extent.h). The ExtensionExtent should contain: - All the URLPatterns from Extension::host\_permissions\_ - All the URLPatterns from all the matches from all the content scripts. The path component of these URLPatterns should be set to "/". - The code that is currently there does the above two steps, but instead of returning URLPatterns, it condenses the information down into just the hosts. That part is only needed by the Install UI, and should move to extension\_install\_ui.cc somewhere. 2. Take a look at ExtensionInfo in chrome\_url\_request\_context.h. Add an effective\_host\_permissions field and populate it from Extension::GetEffectiveHostPermissions() similarly to how the others are done. 3. In extension\_protocols.cc, there are some other checks similar to the one you want to do in CreateExtensionURLRequestJob. Use context.effective\_host\_permissions.ContainsURL() to decide whether to block a resource load. Note that this is only checking whether the extension being requested \_could\_ run code in the page. Checking whether the extension \_did\_ run code in the page is much more complicated and would probably involve upstream changes to keep track of whether any injections had been done.

## Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=45876>

## Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=56215&view=revision>

## CVE-2010-2110

### Context

Related to when the extensions modify a Web page's DOM tree.

Google Chrome before 5.0.375.55 does not properly execute JavaScript code in the extension context, which has unspecified impact and remote attack vectors.

### Problem

Summary: Inappropriate context isolation of the "Tabs" world and the "extensions" world. Details: If an extension causes DOM event to be fired (e.g. by modifying DOM tree, which is rather common, or explicitly calling dispatchEvent), the event listener installed by the main page will be erroneously called in extension's context. While actual handler code will be executed in context associated with the JS function (hence in page's world), JS wrappers for DOM objects will be retrieved from extension's

world. This allows a malicious page to mess with extension's Object.prototype by following prototype chain of any DOM object -- e.g. by installing property getters/setters there. Data sent to/from background page may sometimes be intercepted and extension's logic altered. Note that the extent appears to be limited to DOM object prototypes -- the page handler still runs in page's world, and whatever code it may trick extension to execute by modifying prototypes, will still be running in page's context.

#### Solution

```
Changed its Javascript engine (V8) to check the context of the event to know where to dispatch the event: 48 v8::Local WorldContextHandle::adjustedContext(V8Proxy* proxy) const 49 { 50 if (m_worldToUse == UseMainWorld || !m_context || m_context->get().IsEmpty()) 51 return proxy->mainWorldContext(); 52 53 return v8::Local::New(m_context->get()); 54 }
```

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=42228>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=45686&view=revision>

## CVE-2010-2108

#### Context

When the user blocks certain plug-ins to be executed it allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.

#### Problem

Plugins are not always blocked by content settings.

In Chromium, users are allowed to select certain Websites that are authorized to load plugins into the browser. The problem in this CVE is that it allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.

Repro steps:

1- Modify content settings to block all plugins

2- Load test case

3- Click button

4- Notice that the plugin loads and can be played

The bug is likely related to the fact that we only send down the blocked content settings in response to a top-level navigation. In this example, there is no top-level navigation since the newly opened window is to about:blank.

#### Solution

The key here is to realize that the newly-created window doesn't have a host, and thus no host-based settings could apply to it. And the only way for it to get a host is to navigate, at which time we'll pass the right setting for the new host. Therefore, the only settings that can apply are the global defaults. That suggests the fix: when the renderer wants to create a new view, it sends an IPC to the browser; at that time, we should pass down the default settings so the renderer can apply them to the new view. We can use our existing IPC for this. This should be a small fix so we can merge it to the branch even after the feature freeze, but if anyone wants to do it now they're welcome.

#### Issue Tracking URL

- <https://bugs.chromium.org/p/chromium/issues/detail?id=39740> <https://googlechromereleases.blogspot.com/2010/05/stable-channel-update.html>

#### Commit URL

- <https://src.chromium.org/viewvc/chrome?revision=43792&view=revision>

## CVE-2010-1229

#### Context

Sandbox Infrastructure (IPC mechanism) in Google Chrome before 4.1.249.1036 does not properly use pointers, which has unspecified impact and attack vectors.

#### Problem

A compromised renderer can pass an arbitrary pointer to the plugin process; this pointer is then dereferenced and manipulated (written) in the plugin process. This could be used to corrupt the plugin process and execute arbitrary code outside the sandbox.

Steps to reproduce:

1. Create a plugin.htm page with the following (this just loads the Acrobat plugin so you can mess with it):

```
<body>
    <embed id="pdf" type="application/pdf" hidden="true" width="0" height="0"></embed>
</body>
<script>
    var obj = document.getElementById("pdf");
    var x = new Object();
    obj.messageHandler = x;
</script>
```

2. Set a breakpoint in the renderer process on ParamTraits::Write()

3. Attach to the renderer process and load plugin.htm.

4. After breaking, change the value of p.type to 7 (which is NPVARIANT\_PARAM\_OBJECT\_POINTER; it should initially be 6, which is NPVARIANT\_PARAM\_OBJECT\_ROUTING\_ID).

5. Change the value of p.npobject\_pointer to 0x41414141 (or any garbage value) to trigger a crash on a write violation in the plugin process. The plugin process will read the supplied value with ParamTraits::Read() and treat it as an NPObjec pointer. The reference count (address+4 on x86) is incremented shortly after reading, which is why a crash occurs when an invalid address is provided.

Root Cause of the Problem:

The renderer and plugin processes can send over raw NPObjets valid in the other side's address space. Basically, the way this works is if an NPObjec is marshaled over to the other side, an NPObjecStub is created in the caller address space and a NPObjecProxy is created on the other side. The NPObjecProxy is passed the raw NPObjec pointer which is used as a cookie. If the original NPObjec needs to be passed back we pass the underlying NPObjec saved in the NPObjecProxy. The receiver does not validate whether this NPObjec is valid before invoking on it. While this is mostly fine, in the case of a compromised renderer invalid addresses could be passed back to the plugin which would invoke on these addresses and crash.

**Solution**

Fix is to never pass raw object pointers across and just pass the corresponding routing id of the NPObjecStub. The receiver validates this object by invoking a new method GetNPObjecListenerForRoute on the PluginChannelBase. This method returns the corresponding NPObjec listener for the routing id. We then retrieve the underlying NPObjec from the listener and use it. The map of NPObjecListeners which is maintained by PluginChannelBase has been changed to hold NPObjecBase pointers instead. NPObjecStub and NPObjecProxy implement the new NPObjecBase interface which provides methods to return the underlying NPObjec and the IPC::Channel::Listener pointer.

**Issue Tracking URL**

- <https://bugs.chromium.org/p/chromium/issues/detail?id=28804>
- <https://bugs.chromium.org/p/chromium/issues/detail?id=31880>

**Commit URL**

- <https://src.chromium.org/viewvc/chrome?revision=38725&view=revision>
- <https://src.chromium.org/viewvc/chrome?revision=37555&view=revision>

# Firefox

## CVE-2016-1966

### Context

When Firefox handles NPAPI plug-ins that create multiple objects of type NPObj that needs to be wrapped with an Object Wrapper.

### Problem

We believe there to be an incorrect assumption regarding the purpose of a certain variable assignment which is assumed to be obsolete. The 'entry' variable is a pointer to an entry inside the data storage of the global 'sNPObjWrappers' (which keeps track of the object wrappers used in the application). This may cause the NPAPI subsystem to crash. The high-level PoC to trigger the vulnerability and cause a crash is as follows:

1. write a NPAPI plug-in which has a function that creates and returns a new NPObj every time it is called; 2. call that function in a loop from Javascript. The browser will likely crash when a HashTable Object resizes its underlying data storage."

### Solution

Fix an erroneous nsNPObjWrapper assertion.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1246054](https://bugzilla.mozilla.org/show_bug.cgi?id=1246054)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8716183>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8720113>

## CVE-2016-1949

### Context

Mozilla Firefox before 44.0.2 does not properly restrict the interaction between Service Workers and plugins, which allows remote attackers to bypass the Same Origin Policy via a crafted web site that triggers spoofed responses to requests that use NPAPI, as demonstrated by a request for a crossdomain.xml file.

### Problem

NPAPI-initiated network requests can be intercepted by service workers, hence breaking plugin origin expectations

### Solution

Make plugin network requests bypass service worker interception

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1245724](https://bugzilla.mozilla.org/show_bug.cgi?id=1245724)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8717515>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8716984>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8717114>

## CVE-2016-1948

### Context

Mozilla Firefox before 44.0 on Android does not ensure that HTTPS is used for a lightweight-theme installation, which allows man-in-the-middle attackers to replace a theme's images and colors by modifying the client-server data stream.

### Problem

To install a lightweight theme, we listen for custom events from addons.mozilla.org, and we check the document URI to make sure these events are actually coming from addons.mozilla.org. However, we don't check the scheme to ensure it's https. This creates the opportunity for a malicious party to spoof the DNS entry for http://evil.addons.mozilla.org/ and from there still act with the same privileges as https://addons.mozilla.org/ and install themes.

### Solution

Add the HTTPS check for schemes.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1235876](https://bugzilla.mozilla.org/show_bug.cgi?id=1235876)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8702984>

## CVE-2015-7223

### Context

The WebExtension APIs in Mozilla Firefox before 43.0 allow remote attackers to gain privileges, and possibly obtain sensitive information or conduct cross-site scripting (XSS) attacks, via a crafted web site.

### Problem

Firefox doesn't check that a document belongs to an extension before injecting APIs into it. In the case of background pages, it continues injecting APIs into new window globals even after the first load. This means that if a background page navigates to a remote web page, that page has the full privileges of the extension. Remote URLs loaded into popups get the same elevation of privileges too.

### Solution

Don't inject WebExtension APIs into documents without WebExtension principals

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1226423](https://bugzilla.mozilla.org/show_bug.cgi?id=1226423)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8692227>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8690345>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8690289>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8690290>

## CVE-2015-7196

#### Context

Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4, when a Java plugin is enabled, allow remote attackers to cause a denial of service (incorrect garbage collection and application crash) or possibly execute arbitrary code via a crafted Java applet that deallocates an in-use JavaScript wrapper.

#### Problem

A Java Plugin destroys an object in a thread other than the main thread, which causes its buffer store entry not to be removed in the main thread. This causes the GC to crash when it encounters the buffer store entry.

It possible result in arbitrary code execution via a crafted Java applet that deallocates an in-use JavaScript wrapper.

#### Solution

Add a MOZ\_CRASH if the thread where the object is destroyed is not the main one.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1140616](https://bugzilla.mozilla.org/show_bug.cgi?id=1140616)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8646867>

## CVE-2015-7187

#### Context

The Add-on SDK in Mozilla Firefox before 42.0 misinterprets a "script: false" panel setting, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via inline JavaScript code that is executed within a third-party extension.

#### Problem

When creating extensions, if it specifies that it will not use JS (allow: { script: false }), it can still write in-line JS code in HTML pages which will be executed. This means that attackers can perform XSS attacks through in-line JS in extensions. The problem was apparently in a default true to allow inline JS

Steps to reproduce:

1. Create a browser extension for Firefox.

2. Create a panel with script: false:

```
function createPanel () {
    var sd = require("sdk/self").data;
    myPanel = require("sdk/panel").Panel({
        width: 640,
        height: 522,
        allow: { script: false },
        contentScriptFile: [ sd.url("full.js"), sd.url("popupscript.js") ]
```

3. Pull an external html page into the panel and include: <script>alert('this shouldnt happen');</script>

Issue was found on firefox 40, but I believe it exists prior.

Actual results:

Alert box with "this shouldnt happen" appears.

Expected results:

Inline script should have been ignored due to this flag:

```
allow: { script: false }
```

#### Solution

Check for the allow script specification before running any sort of JS.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1195735](https://bugzilla.mozilla.org/show_bug.cgi?id=1195735)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8668491>

## CVE-2015-4498

#### Context

The add-on installation feature in Mozilla Firefox before 40.0.3 and Firefox ESR 38.x before 38.2.1 allows remote attackers to bypass an intended user-confirmation requirement by constructing a crafted data: URL and triggering navigation to an arbitrary http: or https: URL at a certain early point in the installation process.

#### Problem

When the page is redirecting or navigating by ana href link, JavaScript or server redirect, Firefox throws the 'Firefox prevented this site (site.com) from asking you to install software on your computer.' warning at the user, which needs to explicitly be accepted for the add-on to continue installing.

There is, however, a simple vulnerability that lets an attacker bypass this dialog, which allows a rather nasty attack on the user.

Basically, there is one exception in which the dialog will not be shown, which is if the user pastes or copies the direct link/URL in the URL bar. The user could also just

click on links, redirects etc that lead to this page, because a data uri redirected to the page which itself redirects with a 'page moved header' to the location of the add-on, will disrupt that 'chain' and installation of the add-on will start without the dialog, as if the user typed it in directly.

#### Solution

Check that the triggeringPrincipal subsumes the principal of the document loaded in the tab that started the install. The fix is to block cross-origin add-on install requests.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1042699](https://bugzilla.mozilla.org/show_bug.cgi?id=1042699)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8652099>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8652514>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8652513>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8652680>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8651890>

## CVE-2015-4495

#### Context

PlayPreview (PDF Viewer)

The PDF reader in Mozilla Firefox before 39.0.3, Firefox ESR 38.x before 38.1.1, and Firefox OS before 2.2 allows remote attackers to bypass the Same Origin Policy, and read arbitrary files or gain privileges, via vectors involving crafted JavaScript code and a native setter, as exploited in the wild in August 2015.

#### Problem

Security researcher Cody Crews reported on a way to violate the same origin policy and inject script into a non-privileged part of the built-in PDF Viewer.

This exploit allows attackers to read and copy information on victim's computer, once they view the web site crafted with this exploit.

Proof of Concept: Create a index.html and copy and paste the following html into it:

Test: Run the index.html (Make sure the main.js is in the same directory) and we should be able to see the directory listing.

#### Solution

WIP disables native PDF plugins (In reply to Boris Zbarsky [:bz] from comment #1)

"So I tried to hack on this last night but discovered that at least on my Mac > we're treating the Adobe PDF plug-in as always disabled, which is not very > helpful for debugging.

If you can tell me how to detect the "internal PDF viewer is enabled" state,

I can try to put up some patches that implement this proposal for testing... The PDF viewer detects if it is enabled via multiple configuration flags. See

<http://mxr.mozilla.org/mozilla-central/source/browser/extensions/pdfjs/content/PdfJs.jsm#275>. I think the best way to detect if PDF viewer is enabled is to check stream converter. I created a WIP patch (see attachment) -- I will check if the test page works on Windows with internal PDF viewer on/off soon. Remove PlayPreview usage from PDF viewer"

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1178058](https://bugzilla.mozilla.org/show_bug.cgi?id=1178058)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1179262](https://bugzilla.mozilla.org/show_bug.cgi?id=1179262)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8628914>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8643943>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8643945>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8644113>

## CVE-2015-2709

#### Context

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 38.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

#### Problem

A missing nullptr check in GetDocument and a missing check of the content pointer before initializing instanceOwner cause Firefox to crash.

#### Solution

Add null check

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1111251](https://bugzilla.mozilla.org/show_bug.cgi?id=1111251)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1155474](https://bugzilla.mozilla.org/show_bug.cgi?id=1155474)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1143194](https://bugzilla.mozilla.org/show_bug.cgi?id=1143194)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1117977](https://bugzilla.mozilla.org/show_bug.cgi?id=1117977)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1146101](https://bugzilla.mozilla.org/show_bug.cgi?id=1146101)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1135066](https://bugzilla.mozilla.org/show_bug.cgi?id=1135066)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1149526](https://bugzilla.mozilla.org/show_bug.cgi?id=1149526)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1128064](https://bugzilla.mozilla.org/show_bug.cgi?id=1128064)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1153688](https://bugzilla.mozilla.org/show_bug.cgi?id=1153688)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8593079>

## CVE-2015-2706

#### Context

Race condition in the AsyncPaintWaitEvent::AsyncPaintWaitEvent function in Mozilla Firefox before 37.0.2 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via a crafted plugin that does not properly complete initialization.

#### Problem

Failed initialization of the plugins causes a race condition, because the destroyer of an object linked to the plugin is not called, which causes the potential for UAF.

#### Solution

Destroy the owner object - related to the plugin - if the plugin fails to initialize.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1141081](https://bugzilla.mozilla.org/show_bug.cgi?id=1141081)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8589247>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8582844>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8590374>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8579081>

## CVE-2015-0812

#### Context

Mozilla Firefox before 37.0 does not require an HTTPS session for lightweight theme add-on installations, which allows man-in-the-middle attackers to bypass an intended user-confirmation requirement by deploying a crafted web site and conducting a DNS spoofing attack against a mozilla.org subdomain.

#### Problem

Extended browser access is granted to some Mozilla-owned domains, such as addon management for addons.mozilla.org, which is defined by the default\_permissions file, as I understood it. But unlike the "UITour" permissions granted for www.mozilla.org, this API is not restricted to the https:// protocol. This should not be a security risk per se, since addons.mozilla.org provides HSTS headers and is included in the static HPKP pinning list anyways, which should render any attempt to tamper with plain HTTP traffic impossible. Nevertheless sub-subdomains do not seem to enforce SSL here. So a MITM can spoof the DNS entry for http://evil.addons.mozilla.org/ and from there still act with the same privileges as https://addons.mozilla.org/.

#### Solution

Add the HTTPS check for schemes. Side note: Comment #2: "AFAIK, the only reason not to enforce that are historical - changing it may break existing legitimate 3rd party install sites. And specialized cases like enterprise environments, I guess - but I don't have any data to back that up (and we can work around that anyway). We do perform a reasonably strict HTTPS check in the install phase, but we allow a bypass using a hash check. That's designed for a MitM of the actual install file, not the install request. If a MitM can control the install request site, then it would likely be pointing at a file on a site it controls anyway - so our checks in the install phase won't help. I think the benefits outweigh the costs of what we may break. Saying that, needinfo on Dave in case he has more historical context around this. In the mean time, I'll work up a patch."

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1128126](https://bugzilla.mozilla.org/show_bug.cgi?id=1128126)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8561128>

## CVE-2014-8643

#### Context

Mozilla Firefox before 35.0 on Windows allows remote attackers to bypass the Gecko Media Plugin (GMP) sandbox protection mechanism by leveraging access to the GMP process, as demonstrated by the OpenH264 plugin's process.

#### Problem

The sandboxed plugin-container.exe process on Windows holds a handle to the parent process. While the access rights on this handle are somewhat limited (0x101441) it still allows us to duplicate handles in the parent process (PROCESS\_DUP\_HANDLE). Using DuplicateHandle we can issue a call that duplicate the process handle from the parent process to our current process (-1 a pseudo handles to the parent and current (sandboxed process). The call will succeed and a new handle to the parent process is created in the sandboxed child. This handle has full access to the parent which then allows for executing arbitrary code in the parent through CreateRemoteThread.

#### Solution

Do not allow calls to OpenProcess function, which allows handles to be duplicated, after user content has been loaded.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1117140](https://bugzilla.mozilla.org/show_bug.cgi?id=1117140)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8545254>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8544691>

## CVE-2014-1519

#### Context

PluginModuleParent may delete its subprocess before calling MessageChannel::Clear, resulting in badness

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0 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.

#### Problem

1) PluginModuleParent contains a PluginProcessParent, mSubprocess. When PluginModuleParent is created by static ::LoadModule, it passes parent->mSubprocess->GetChannel() to parent->Open(). [A] 2) PluginModuleParent::Open(), calls PluginModuleParent->mChannel->Open(), which is a MessageChannel. 3) MessageChannel::Open creates a ProcessLink, mLink, and passes it the channel from the subprocess in (1) [B] 4) NP\_Initialize returns an error from the plugin. We set mShutdown = true without actually calling NP\_Shutdown. [E] There are a few other pathways that do something similar [C] [D] (maybe [F], but the callers I checked are caused by channel shutdown) 5) We decide to destroy PluginModuleParent, and call in order: - ~PluginModuleParent - mSubprocess->Destroy() - ~MessageChannel (PluginModuleParent.mChannel destructor) - MessageChannel::Clear - delete mLink - ~ProcessLink - mTransport->set\_listener(); mTransport is the channel obtained from mSubprocess in (1) 6) mSubprocess->Destroy() queues a task on the io thread to run [delete this]. This task then races with us getting to MessageChannel::Clear. If it wins the race, MessageChannel.mLink now has a poisoned mTransport, and we crash. This can be reproduced in a debugger by breaking at [G] and [E]. Fudge the plugin return code at [E]\* and stop the main thread at [G] so the iothread wins the race. Backtrace attached, which appears identical to the bug 974933 crashes: <https://crash-stats.mozilla.com/report/index/c68aaee10-a11f-4191-ab54-298b12140227> \* I'm not sure about this part -- we can't call NP\_Shutdown or MessageChannel::Clear() will

prevent the race. Any of the abnormal-failure paths that set |mShutdown = true| without calling ::Clear might be triggering this. [A] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#97> [B] <http://dxr.mozilla.org/mozilla-central/source/IPC/glue/MessageChannel.cpp#296> [C] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#1196> [D] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#111> [E] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#1228> [F] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginProcessParent.cpp#82>

#### Solution

Close the channel when aborting before successful init So mShutdown tracks if our channel has died, and the destructor calls NP\_Shutdown if it has not. This is circumvented, however, by error paths that set it to true during init to indicate that NP\_Shutdown shouldn't be called. All of these paths except one in LoadModule also leave the channel open erroneously, so just calling Close() when we want to shutdown without calling the plugin should fix the issue. The one case in LoadModule sets mShutdown because the object dies before calling Open(). It doesn't look like there's a sane way to assert that MessageChannel was cleaned up -- double-calling Close() is a runtime abort, and MessageChannel::Connected() doesn't guarantee we're not somewhere between closed and connected (and is private anyway). Is there an assertion we could add to the destructor, or is it worth modifying MessageChannel to add one? Given that this patch restores mShutdown to properly track the "After Open() before Close()" state I'm fairly confident this can't happen in other ways in the existing code at least.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=996883](https://bugzilla.mozilla.org/show_bug.cgi?id=996883)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=919592](https://bugzilla.mozilla.org/show_bug.cgi?id=919592)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=995607](https://bugzilla.mozilla.org/show_bug.cgi?id=995607)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=990794](https://bugzilla.mozilla.org/show_bug.cgi?id=990794)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=946658](https://bugzilla.mozilla.org/show_bug.cgi?id=946658)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=953104](https://bugzilla.mozilla.org/show_bug.cgi?id=953104)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=986864](https://bugzilla.mozilla.org/show_bug.cgi?id=986864)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=977955](https://bugzilla.mozilla.org/show_bug.cgi?id=977955)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8385637>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8385636>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8383965>

## CVE-2013-1713

#### Context

In the plugin extensions (when checking the principal when validating URI loads of extensions )

#### Problem

The InstallTrigger component can use the wrong principal when validating URI loads. It was happening because this component was grabbing the origin information from the outer window. This is a potential concern in other javascript components that use the document of the window they're accessible from to perform checks against URLs before performing sensitive actions, and could also potentially be used to bypass the same origin policy and other all around nastiness.

#### Solution

Fix is to get the principal information from the right context.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=887098](https://bugzilla.mozilla.org/show_bug.cgi?id=887098)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=768106>
- <https://bugzilla.mozilla.org/attachment.cgi?id=767910>

## CVE-2013-0798

#### Context

Mozilla Firefox before 20.0 on Android uses world-writable and world-readable permissions for the app\_tmp installation directory in the local filesystem, which allows attackers to modify add-ons before installation via an application that leverages the time window during which app\_tmp is used.

#### Problem

The installation of the Firefox for Android (FFA) makes app\_tmp directory world readable and writable(777). With this configuration other applications (might be malicious) can replace any addons installed through FFA. This leads installing mal-addons without any awareness from users.

#### Solution

move the about:memory dumps to somewhere on /sdcard (change the tmp directory) and set the right permissions. Note: It's complicated in Android to change permissions for existing directories, that's why the workaround (delete the old one and create a new one with the right permissions)

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=844832](https://bugzilla.mozilla.org/show_bug.cgi?id=844832)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=723633>
- <https://bugzilla.mozilla.org/attachment.cgi?id=718433>

## CVE-2013-0747

#### Context

Can confuse PluginHandler Event by listening for mutation events.

#### Problem

JavaScript error: chrome://browser/content/browser.js, line 10437: iconStatus is null

```

>         let installStatus = doc.getAnonymousElementByAttribute(plugin, "class", "installStatus");
>         installStatus.setAttribute("status", "ready");
>         let iconStatus = doc.getAnonymousElementByAttribute(plugin, "class", "icon");
>         iconStatus.setAttribute("status", "ready");

```

The page gets an event whose originalTarget is an anonymous DIV. It is not expected that the page be able to get a reference to the anonymous content. • Content pages shouldn't be able to access native anon content. There used to be an exception if that happened. A dedicated attacker could turn it into something pretty serious by rearranging the anonymous DOM and clickjacking plugin install prompts.

#### Solution

The fix was to add a <binding native="true"> attribute which would force the pluginProblem XBL subtree to be considered native-anonymous instead of just anonymous, which would prevent access from content script.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=733305](https://bugzilla.mozilla.org/show_bug.cgi?id=733305)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=662337>
- <https://bugzilla.mozilla.org/attachment.cgi?id=694813>

## CVE-2012-4194

#### Context

Location can be spoofed using |valueOf|

#### Problem

When Adobe Flash Player checks the page location to apply the SOP (Same-Origin Policy), it reads the return value of javascript:top.location+"\_\_flashplugin\_unique\_\_". When an object is joined with a string, its |valueOf| method is called before |toString|, and content can redefine the former. This appears to have regressed in Firefox v16.0.1.

In short, the property can be altered to gain access to attributes that are not supposed to be accessed.

#### Solution

Prevent shadow of built-in location.valueOf.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=800666](https://bugzilla.mozilla.org/show_bug.cgi?id=800666)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=674879>

## CVE-2012-3994

#### Context

Using Object.defineProperty to interfere with other add-ons (or the application).

#### Problem

The `Object.defineProperty` can shadow `|top|`. Plugins may try to access it through `|top.location|` -- for instance, Adobe Flash Player opens `javascript:top.location+"__flashplugin_unique__"` to determine the page origin. And it is possible to shadow `|top|` using `Object.defineProperty`. Incidentally, Google Chrome seems to disallow redefining `|top|`.

#### Solution

Reload Iframe and re-create docshell

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=765527](https://bugzilla.mozilla.org/show_bug.cgi?id=765527)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=650991>

## CVE-2012-3975

#### Context

The created document is a data document, so it itself shouldn't load anything. HTML parser may speculatively load something. (It shouldn't enable speculative loads for data documents)

#### Problem

This is a bad bug in the patch for bug 102699. Before that patch, the only codepath that could lead to parsing looked like this, in order: 1) Create a document with the DOMParser's mOriginalPrincipal. 2) Call EnableXULXBL() on the document if needed 3) Call StartDocumentLoad() 4) Set the document's base URI 5) Reset the document's principal to mPrincipal. 6) Feed data into the parser. That sequence of steps was pretty clearly documented (at least in terms of the whole principal dance) and \_very\_ critical. When that bug was fixed, the XML codepath stayed as above, but HTML codepath was written more like this: 1) Create a document with the DOMParser's mOriginalPrincipal. 2) Feed data into the parser. 3) Call EnableXULXBL() on the document if needed 4) Set the document's base URI 5) Reset the document's principal to mPrincipal. But the whole point of resetting to mPrincipal is that it **MUST** happen before any data goes in. Otherwise you're parsing with the system principal. Also, this is never calling StartDocumentLoad, so afaict it's not setting up whatever state that would normally set up (e.g. the document URI) the same way as the XML path. And it's calling EnableXULXBL() too late, of course. Not like this matters much for text/html. This bug means that using DOMParser on text/html is pretty unsafe from chrome: It allows whatever string you're parsing to poke any URI it wants, including ones that web content normally can't access. (On a Unix system it allows at minimum a DoS attack by reading from file:///dev/tty.)

#### Solution

make sure chrome DOMParser doesn't load external resources

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=770684](https://bugzilla.mozilla.org/show_bug.cgi?id=770684)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=640187>

## CVE-2012-3973

### Context

The debugger in the developer-tools subsystem in Mozilla Firefox before 15.0, when remote debugging is disabled, does not properly restrict access to the remote-debugging service, which allows remote attackers to execute arbitrary code by leveraging the presence of the `HTTPMonitor` extension and connecting to that service through the `HTTPMonitor` port.

### Problem

If remote debugging is disabled, but `HTTPMonitor` is enabled, a remote user can connect to and use the remote debug service.

### Solution

having the server code take the remote-enabled flag into consideration before opening the socket.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=757128](https://bugzilla.mozilla.org/show_bug.cgi?id=757128)

### Commit URL

---

## CVE-2012-3960

### Context

During deallocation

### Problem

Use-after-free vulnerability in `mozSpellChecker::SetCurrentDictionary`. `mozSpellChecker::SetCurrentDictionary` gets called, and then `mozHunspell::SetDictionary` gets called (which is inlined), which in turn calls into the notification service: . The editor then catches that notification and calls `nsEditor::SyncRealTimeSpell`, which can potentially lead into `mInlineSpellChecker` to get set to null , which in turn releases its `mSpellChecker` member , which is a `mozSpellChecker` which we see on the 1st frame of the freeing call stack. Then, all of this stuff returns, and when we get back to the `mozSpellChecker::SetCurrentDictionary` frame, "this is dead, so any attempt to call it (such as calling `Release` on it) will dereference freed memory. Now, I \_think\_ that you can't put arbitrary stuff on the stack between the time that the `mozSpellChecker` object dies and the time that `mozSpellChecker::SetCurrentDictionary` returns, but if I'm wrong, and you could do that, then this gives you a very nice remote exploit, because the offset of `Release` in the vtable is pretty well known...

### Solution

Part 1: Make sure that `mozSpellChecker`'s refcount doesn't go down prematurely; Part 2: Make sure that `nsEditorSpellCheck`'s refcount doesn't go down prematurely;  
Part 3: Make sure that `nsEditorSpellCheck`'s refcount doesn't go down prematurely;

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=771976](https://bugzilla.mozilla.org/show_bug.cgi?id=771976)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=641142>
- <https://bugzilla.mozilla.org/attachment.cgi?id=642856>
- <https://bugzilla.mozilla.org/attachment.cgi?id=643240>

## CVE-2012-1956

### Context

It occurs when extensions manipulate the `Object.defineProperty` as a method to shadow the `location` object (aka `window.location`)

### Problem

It is possible to shadow the `location` object using `Object.defineProperty`. This could be used to confuse the current location to plugins, allowing for possible cross-site scripting (XSS) attacks. It means that an attacker can confuse Flash (or other plugins) into thinking that we're on one domain when, in reality, we're on another one leading to XSS attacks.

### Solution

Create a function that does security checks specifically for the object (`js::CheckDefineProperty(JSContext *cx, HandleObject obj, HandleId id, HandleValue value, PropertyOp getter, StrictPropertyOp setter, unsigned attrs)`).

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=756719](https://bugzilla.mozilla.org/show_bug.cgi?id=756719)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=667903>
- <https://bugzilla.mozilla.org/attachment.cgi?id=634237>

## CVE-2012-0446

### Context

It occurs when frame scripts that call untrusted objects.

### Problem

Frame scripts bypass `XPConnect` security checks when calling untrusted objects. This allows for cross-site scripting (XSS) attacks through web pages and Firefox extensions. Frame scripts run on the special JS context for which we call `SetSecurityManagerForJSContext` with `flags=0`, thus if a frame script calls into an untrusted function, `XPConnect` does not do proper security checks.

### Solution

The fix enables the Script Security Manager (SSM) to force security checks on all frame scripts.

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=705651](https://bugzilla.mozilla.org/show_bug.cgi?id=705651)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=577960>
- <https://bugzilla.mozilla.org/attachment.cgi?id=577535>
- <https://bugzilla.mozilla.org/attachment.cgi?id=578220>

**CVE-2011-3004****Context**

The JSSubScriptLoader in Mozilla Firefox 4.x through 6 and SeaMonkey before 2.4 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.

**Problem**

When loading JS from add-ons, Firefox unwraps the wrapper objects and the code that is supposed to receive a wrapped window, it's now handed the underlying Window allowing that Window's code to possibly catch things like expando sets and then inject its own code into the privileged call

**Solution**

Use a Chrome sandbox object when loading unprivileged JS code

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=653926](https://bugzilla.mozilla.org/show_bug.cgi?id=653926)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=545794>
- <https://bugzilla.mozilla.org/attachment.cgi?id=570350>
- <https://bugzilla.mozilla.org/attachment.cgi?id=546651>

**CVE-2011-3001****Context**

It occurs as part of a user-assisted attack. If you could convince a user to hold down the Enter key--as part of a game or test, perhaps--a malicious page could pop up a download dialog where the held key would then activate the default Open action.

**Problem**

For some file types this would be merely annoying (the equivalent of a pop-up) but other file types have powerful scripting capabilities. And this would provide an avenue for an attacker to exploit a vulnerability in applications not normally exposed to potentially hostile internet content. There are 2 layers of protection against an unauthorized installation of extensions: 1) The principal of the opener is checked against whitelisted domains that are allowed to download the plugin without asking. If the domain is not trusted, the user is asked to allow to download the plugin. 2) When the plugin is downloaded, the user is asked to confirm the installation. The first protection can be circumvented by creating a hidden "Embed" element containing an arbitrary XPI as its "pluginspage" parameter. The attacker can focus this element while the user holds Enter, causing a number of "Plugin Finder Service" windows to appear. The first window focuses the "Cancel" button and will just close, but all the subsequent ones will set focus on the "Manual Install" button directing to the malicious XPI. As soon as the user releases the key, the browser will start launching multiple windows with the provided URL. The windows will have a ChromeWindow object as their opener, so the user will not be asked to allow to download a plugin. The second protection can be bypassed due to a logic error in amWebInstallListener.js. When no window-watcher is registered in Services, this will throw:

**Solution**

It ensures that window watcher is defined, such that it can show the install dialog.

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=672485](https://bugzilla.mozilla.org/show_bug.cgi?id=672485)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=555021>

**CVE-2011-2370****Context**

Mozilla Firefox before 5.0 does not properly enforce the whitelist for the xpinstall functionality, which allows remote attackers to trigger an installation dialog for a (1) add-on or (2) theme via unspecified vectors.

**Problem**

In the install functionality, it's possible to redefine window.location. Thus, content code can control this.window.location.href. Moreover, this.window is not being wrapped.

**Solution**

Stops using the unwrapped window and also switches to using document.documentElementObject throughout the installation process.

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=645699](https://bugzilla.mozilla.org/show_bug.cgi?id=645699)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=523069>

**CVE-2011-0076****Context**

## Sandbox

Unspecified vulnerability in the Java Embedding Plugin (JEP) in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, on Mac OS X allows remote attackers to bypass intended access restrictions via unknown vectors.

### Problem

Vulnerability in the Java Embedding Plugin (JEP) on Mac OS X allows remote attackers to bypass intended access restrictions via unknown vectors.

We have discovered a vulnerability in the JEP or LiveConnect java bridge in Firefox. We initially investigated this as a bug in the Java distribution, but it now seems to be a Mozilla-specific problem. Therefore I'm giving you the proof-of-concept so that you can investigate further. ===== javafs.html ===== cut ===== 1. Put javafs.html (contents per the above) on a web server. 2. Visit that page in Firefox. 3. Note how the script was permitted to get a reference to the java.io.FileSystem class, even though it is declared package-local. I reproduced the issue with Firefox 3.6.13.

### Solution

Not provided

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=634724](https://bugzilla.mozilla.org/show_bug.cgi?id=634724)
- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=644682](https://bugzilla.mozilla.org/show_bug.cgi?id=644682)

### Commit URL

---

## CVE-2010-1585

### Context

During Plug-ins execution (protection mechanism against unsafe javascript).

### Problem

The two ns(X)HTMLParanoidFragmentSink classes are used by nsIScriptableUnescapeHTML to sanitize (X)HTML by stripping attributes and tags not on a built-in whitelist. It allows javascript: URLs and other inline JavaScript when the embedding document is a chrome document. While there are no unsafe uses of this class in any released products, extension code could have potentially used it in an unsafe manner. The sinks attempt to sanitize URLs by calling CheckLoadURI[...]DISALLOW\_INHERIT\_PRINCIPAL, but unfortunately when the target document is a chrome document (as is common with add-ons) this check allows any URI. In particular malicious href="javascript:evil()" or <frame src="data:evil"> can slip through and create sg-critical bugs. In short, it 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.

### Solution

DISALLOW\_INHERIT\_PRINCIPAL always returned "ok" for system principals. Therefore, they used a null principal when performing the validation.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=562547](https://bugzilla.mozilla.org/show_bug.cgi?id=562547)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=442465>
- <https://bugzilla.mozilla.org/attachment.cgi?id=497538>
- <https://bugzilla.mozilla.org/attachment.cgi?id=497566>
- <https://bugzilla.mozilla.org/attachment.cgi?id=499199>

## CVE-2010-1198

### Context

Use-after-free vulnerability allows remote attackers to execute arbitrary code via vectors involving multiple plugin instances. Deallocator A flaw was discovered in the way plugin instances interacted. An attacker could potentially exploit this and use one plugin to access freed memory from a second plugin to execute arbitrary code with the privileges of the user invoking the program.

### Problem

two plugin instances could interact in a way in which one plugin gets a reference to an object owned by a second plugin and continues to hold that reference after the second plugin is unloaded and its object is destroyed. In these cases, the first plugin would contain a pointer to freed memory which, if accessed, could be used by an attacker to execute arbitrary code on a victim's computer.

### Solution

instead of unwrapping an NPObj which is passed to a different instance (NPP), we should double-wrap it. This means that the other plugin would obtain a reference to a nsJSObjWrapper, instead of the other-plugin-implemented NPObj\* which is destroyed when the plugin is destroyed.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=532246](https://bugzilla.mozilla.org/show_bug.cgi?id=532246)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=415697>
- <https://bugzilla.mozilla.org/attachment.cgi?id=415695>

## CVE-2010-0179

### Context

When dispatching events from the XMLHttpRequestSpy module (a Firebug add-on)

### Problem

When accessing this.xhrRequest.onreadystatechange, content functions (QueryInterface, getInterfaces, etc.) can be called. In other words, when add-ons try to get a reference to onreadystatechange, we call getInterfaces on the existing handler (through the nsXPCWrappedJS). Since the application does not properly handle interaction between the XMLHttpRequestSpy object and chrome privileged objects, it allows remote attackers to execute arbitrary JavaScript via a crafted HTTP response.

In short: Add-ons can get more information from calling functions they're not supposed to because the application doesn't check for the principal.

### Solution

The fix is to check the correct principal (origin). "If no scripted code is running "above" (or called from) fp, then instead of looking at cx->globalObject, |principal| is returned."

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=504021](https://bugzilla.mozilla.org/show_bug.cgi?id=504021)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=395462>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410791>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410788>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410808>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410809>
- <https://bugzilla.mozilla.org/attachment.cgi?id=423691>
- <https://bugzilla.mozilla.org/attachment.cgi?id=425570>

## CVE-2010-0177

#### Context

frees the contents of the window.navigator.plugins array while a reference to an array element is still active, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to a "dangling pointer vulnerability." window.navigator.plugins

#### Problem

error in the implementation of the window.navigator.plugins object. When a page reloads, the plugins array would reallocate all of its members without checking for existing references to each member. This could result in the deletion of objects for which valid pointers still exist. An attacker could use this vulnerability to crash a victim's browser and run arbitrary code on the victim's machine. Successful exploitation can lead to code execution under the context of the application. This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Mozilla Firefox. User interaction is required to exploit this vulnerability in that a user must be coerced to viewing a malicious document. The specific flaw exists within the way the application implements the window.navigator.plugins array. Due to the application freeing the contents of the array while a reference to one of the elements is still being used, an attacker can utilize the free reference to call arbitrary code. Successful exploitation can lead to code execution under the context of the application. The particular vulnerability occurs within the window.navigator.plugins array. This array is implemented within dom/src/base/nsPluginArray.cpp. Each element of this array contains a reference to the mime types installed by that particular plugin. Upon page reload, the plugin array will reallocate all of its members without explicitly checking the used reference count of each member. If an attacker grabs a reference out of the array, and causes the page to reload itself, the attacker will then have a variable that references data that has been freed by the page refresh.

#### Solution

detach the plugin if the mimeType is not null

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=538310](https://bugzilla.mozilla.org/show_bug.cgi?id=538310)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=425799>

## CVE-2010-0170

#### Context

does not offer plugins the expected window.location protection mechanism, which might allow remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via vectors that are specific to each affected plugin Sandbox

#### Problem

the window.location object was made a normal overridable JavaScript object in the Firefox 3.6 browser engine (Gecko 1.9.2) because new mechanisms were developed to enforce the same-origin policy between windows and frames. This object is unfortunately also used by some plugins to determine the page origin used for access restrictions. A malicious page could override this object to fool a plugin into granting access to data on another site or the local file system. The behavior of older Firefox versions has been restored. We removed some code protecting the location object (on both the document and the window) because it isn't needed anymore for either web content or extensions (web pages are allowed to confuse themselves to their heart's content). In doing this, we forgot that plugins also use location.href to figure out what page they've been embedded in.

#### Solution

restore the code protecting the location object that had been removed

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=541530](https://bugzilla.mozilla.org/show_bug.cgi?id=541530)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=434069>
- <https://bugzilla.mozilla.org/attachment.cgi?id=423080>

## CVE-2009-2665

#### Context

when certain add-ons are enabled, does not properly handle a Link HTTP header, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via a crafted web page, related to an incorrect security wrapper. sandboxing

#### Problem

broken functionality on pages that had a Link: HTTP header when an add-on was installed which implemented a Content Policy in JavaScript, such as AdBlock Plus or NoScript. Mozilla security researcher moz\_bug\_r\_a4 demonstrated that the broken functionality was due to the window's global object receiving an incorrect security wrapper and that this issue could be used to execute arbitrary JavaScript with chrome privileges.

#### Solution

If we already have a wrapper at this point, it might have the wrong parent and scope, so reparent it.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=498897](https://bugzilla.mozilla.org/show_bug.cgi?id=498897)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=383939>
- <https://bugzilla.mozilla.org/attachment.cgi?id=383995>

## CVE-2009-1837

#### Context

Race condition in the NPObjWrapper\_NewResolve function in modules/plugin/base/src/nsJSNPRuntime.cpp in xul.dll might allow remote attackers to execute arbitrary code via a page transition during Java applet loading, related to a use-after-free vulnerability for memory associated with a destroyed Java object. deallocation

#### Problem

A vulnerability was reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create specially crafted HTML that, when loaded by the target user, will navigate away from a web page while a Java applet is loading to cause the applet to be deleted and then later called, potentially writing freed memory and executing arbitrary code on the target system. The code will run with the privileges of the target user. The vulnerability resides in NPObjWrapper\_NewResolve and occurs when accessing the properties of an NPObj. race condition in NPObjWrapper\_NewResolve when accessing the properties of a NPObj, a wrapped JSObject. Balle and Eiram demonstrated that this condition could be reached by navigating away from a web page during the loading of a Java applet. Under such conditions the Java object would be destroyed but later called into resulting in a free memory read. An attacker could potentially write to the freed memory before it is reused and run arbitrary code on the victim's computer.

#### Solution

Find out what plugin (NPP) is the owner of the object we're manipulating, and make it own any JSObject wrappers created here.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=486269](https://bugzilla.mozilla.org/show_bug.cgi?id=486269)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=373405>
- <https://bugzilla.mozilla.org/attachment.cgi?id=370549>

## CVE-2009-1310

#### Context

Cross-site scripting (XSS) vulnerability in the MozSearch plugin implementation allows user-assisted remote attackers to inject arbitrary web script or HTML via a javascript: URI in the SearchForm element.

#### Problem

malicious MozSearch plugin could be created using a javascript: URI in the SearchForm value. This URI is used as the default landing page when an empty search is performed. If an attacker could get a user to install the malicious plugin and perform an empty search, the SearchForm javascript: URI would be executed within the context of the currently open page.

#### Solution

ignore search form urls filter the SearchForm value the same way we already filter templateURI and the IconURL.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=483086](https://bugzilla.mozilla.org/show_bug.cgi?id=483086)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=374772>
- <https://bugzilla.mozilla.org/attachment.cgi?id=367754>

## CVE-2008-5013

#### Context

Mozilla Firefox Flash Player Dynamic Module Unloading Vulnerability Build identifier: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/2008020121 Firefox/2.0.0.12 the POC page runs a lot slower. The HTML content is shown, then the dialogs, but then firefox crashes

#### Problem

Tipping Point has reported a bug in the Flash plugin for Firefox which they claim contains a buffer overflow. This could potentially allow an attacker to execute arbitrary code on victim's computer. Build identifier: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/2008020121 Firefox/2.0.0.12 the POC page runs a lot slower. The HTML content is shown, then the dialogs, but then firefox crashes

#### Solution

This is a backport of the changes we took on the trunk for bug 410946. Given that our plugin initialization code is \*really\* different on the branch compared to trunk the changes to nsObjectFrame.cpp are not back-portable to the branch, but the changes to the plugin code alone seems to fix this particular problem. There's probably still fragility in the plugin frame code that is \*not\* addressed by this patch, and the only likely fix for that on the branch would be to port all the plugin loading changes from the trunk back to the branch, and that's \*really\* not trivial, and I would advice against investing in that given the \*huge\* number of regressions (and changes in functionality) we found from that change on the trunk, years after the change went in.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=433610](https://bugzilla.mozilla.org/show_bug.cgi?id=433610)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=335479>

## CVE-2008-2807

#### Context

Faulty .properties file results in uninitialized memory being used

#### Problem

I have hit a weird bug writing an extension for Firefox. The extension is localized in both french and english. One of the french \*.properties file was not UTF-8 but ISO8859-encoded. The window opened by my extension retrieves 3 strings from that properties file. Surprisingly, the first retrieval (string 'textLayouts' in the attached file) did not fail, while the two others did fail. BUT what I got back from that first |GetStringFromName()| call was absolutely not what's in the properties file but some text coming from a MS Word process also running on my machine !!! My XUL window was showing me a bit of the text I was editing in Word... Fixing the encoding of the file of course resolved the issue.

#### Solution

Very safe fix ensuring that the length returned by UTF8InputStream::Read doesn't exceed the number of characters successfully converted.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=397093](https://bugzilla.mozilla.org/show_bug.cgi?id=397093)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=308810>
- <https://bugzilla.mozilla.org/attachment.cgi?id=307421>

## CVE-2008-2806

#### Context

Mozilla.org distributions on the Mac that can use Java have for some time bundled the Java Embedding Plugin, which allows non-WebKit browsers to use current Java versions on OS X.

#### Problem

The Firefox Mac OS X Java Plugin (MRJ Plugin) is vulnerable to the 'document.domain' bypass. Document.domain gets/sets the domain portion of the origin of the current document, as used by the same origin policy. By using the document.domain exception to the same origin policy, LiveConnect, which is a feature of web browsers which allows Java applets to communicate with the JavaScript engine in the browser, and JavaScript on the web page to interact with applets, can be used to create arbitrary socket connections. The code appears to use nsIPrincipal::GetOrigin(), an interface to a principal, which represents a security context, which takes document.domain into account.

In short, the issue was with how the plugin for Java applets makes calls to javascript and obtains the origin of the domains, bypassing the same origin policy.

#### Solution

The fix was to drop any use of GetOrigin() for Java and use the principal's URI

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=408329](https://bugzilla.mozilla.org/show_bug.cgi?id=408329)

#### Commit URL

---

## CVE-2008-2803

#### Context

When loading scripts from extensions (function: mozIJSSubScriptLoader.LoadScript )

#### Problem

It's unsafe to use mozIJSSubScriptLoader.loadSubScript() with non-chrome urls or chrome urls whose scheme/host part contain uppercase characters. Scripts that are loaded in this way do not use implicit XPCNativeWrappers when accessing content, which is used whenever privileged code is used to access unprivileged code. It is used to create a security wrapper that guarantees that the "native" methods/properties of an object will be called (and not the methods overridden by the webpage). As an example, Google Toolbar uses mozIJSSubScriptLoader.loadSubScript() with file: url, and allows an attacker to run arbitrary code with chrome privileges.

#### Solution

They fixed their logic for obtaining a native object wrapper. The decision of whether the subscript gets XPCNativeWrappers or not will depend on the caller, not the file:// URL.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=418356](https://bugzilla.mozilla.org/show_bug.cgi?id=418356)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=310920>
- <https://bugzilla.mozilla.org/attachment.cgi?id=323747>
- <https://bugzilla.mozilla.org/attachment.cgi?id=310145>

## CVE-2007-3844

#### Context

When handling Privileges of plug-ins

#### Problem

window.open("about:blank"); or content.location = "about:blank"; or about:blank when loaded by chrome in these ways has chrome privileges. This behavior could cause security issues in certain extensions that are thinking that about:blank does not have chrome privileges. Imagine an extension that does: 1. Collect urls from content. 2. Load about:blank. (window.open("about:blank") or content.location = "about:blank") 3. Generate links with the urls and insert those into the about:blank document. When an user clicks a javascript: link in the generated page, the script run with chrome privileges. I'm not sure whether this should be fixed or not. If not, we need to advertise the potential problem. (There is an affected extension on AMO.)

#### Solution

The three hunks of this patch do the following: 1) Never allow chrome-privileged data:, javascript:, or about:blank loads in content docshells. Switch them to inheriting principals instead (which is a no-op for about:blank). This behavior is now consistent across all "normal" ways of loading, whereas before window.location allowed chrome javascript: while the nsIWebNavigation APIs, tabbrowser, and setting "src" on s did not. It's still possible to do such loads via manual invocation of nsLinkHandler, but that's not a scriptable API, and doesn't take a principal pointer anyway (it takes a node). This fixes the window.location aspect of this bug. 2) Don't propagate a system principal as the opener principal to new content windows. This fixes the window.open() aspect of this bug. Note that we need both, because CreateAboutBlankContentViewer doesn't actually do a load. 3) Remove now-redundant code in nsFrameLoader. The only risk here, imo is that this does change the behavior of data: and javascript: URIs loaded from chrome in content windows via window.location. If we want I can try to avoid changing that, but the code would be more complex, and I don't think we want to allow it anyway. The former is certainly not safe.

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=388121](https://bugzilla.mozilla.org/show_bug.cgi?id=388121)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=272411>
- <https://bugzilla.mozilla.org/attachment.cgi?id=272432>

**CVE-2006-6499****Context**

The problem is in the JavaScript Engine ( function: jsdtoa)

**Problem**

When a plugin decreases the float precision (a global configuration) it triggers a bug in the javascript engine. In short, a loop in this engine is controlled by the floating point arithmetic. Since that is flawed (or rather becomes flawed after the precision is reduced), the loop becomes infinite, and it keeps adding characters to the string until it crashes. Detailed report: Crash in jsdtoa after opening a new window. There is some very bad logic in jsdtoa, for the case where the double has no fractional component. File: jsdtoa.c See line 2376 /\* Do we have a "small" integer? \*/ In that case there is a loop that converts the double to a string, one digit at a time. In the loop, it looks at the most significant digit, adds that digit to the string, and then removes the digit from the double value. Then, it multiples the value by 10 so shift the digits over to the left. The problem is that the looping logic is dependent on no floating point error being introduced. But, floating point error is introduced when two doubles of different magnitudes are subtracted, which is done here: 2388: d -= L\*d; The check to exit the loop looks like this: 2410: if (!(d != 10.)) break; It compares the double value to zero. Unfortunately, there is floating point error introduced, and the value of "d" never gets down to zero. Therefore, the loop becomes infinite, and we keep appending characters to the output string, ignoring the specified size of the buffer. ( The buffer size test was done previously, based on the number of digits that it planned to place in the buffer. ). My proposed fix is rather simple. Since we know up front how many digits we have to write out, we can use that number to specify the number of times that we loop, rather than depending on errorless floating point math. See the diff between the original and modified files attached. I changed the "for" line: From: for(i = 1; i++ { To: for(i = 1; i<=k+1; i++) { And, I removed the check on the bottom of the for loop. From: if (!(d != 10.)) break; To: d \*= 10.; Furthermore, the logic that is there is very bad. [Description about other problem cut, will file another bug where necessary.]

**Solution**

They fixed the calculations in the loop. [SIDE NOTE] Even though the bug looks like a simple error logic in a loop, from what I saw in the discussions, if they had used the Chrome's approach of isolating javascript objects, this bug would never be exploited. Why? In Chrome, Javascript objects are different (each plugin has its own JS objects), this means that plugins cannot interfere with each other nor the hosting application. Thus, even if a plug-in had decreased the floating precision, the crash would not occur. So the problem seems more like not properly isolating JS objects between plugins and Thunderbird

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=358569](https://bugzilla.mozilla.org/show_bug.cgi?id=358569)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=245115>

**CVE-2006-2784****Context**

The PLUGINSPAGE functionality in Mozilla Firefox before 1.5.0.4 allows remote user-assisted attackers to execute privileged code by tricking a user into installing missing plugins and selecting the "Manual Install" button, then using nested javascript: URLs. NOTE: the manual install button is used for downloading software from a remote web site, so this issue would not cross privilege boundaries if the user progresses to the point of installing malicious software from the attacker-controlled site.

**Problem**

The patch from the previous advisory can be circumvented if the following two changes are made: 1) The embed element is shown on a javascript page 2) The executed javascript accesses chrome using its full privileges to the opener object This can be exploited using a small amount of user interaction which will likely occur given the right social engineering.

**Solution**

Workaround Do not press the "Manual Install" button on the Firefox plugin finder. Instead use a search engine to find an appropriate plugin for the content. moving some code in nsScriptSecurityManager.cpp.

**Issue Tracking URL**

---

**Commit URL**

- 

**CVE-2005-0752****Context**

Plug-in install

The Plugin Finder Service (PFS) in Firefox before 1.0.3 allows remote attackers to execute arbitrary code via a javascript: URL in the PLUGINSPAGE attribute of an EMBED tag.

**Problem**

When a webpage requires a plugin that is not installed the user can click to launch the Plugin Finder Service (PFS) to find an appropriate plugin. If the service does not have an appropriate plugin the EMBED tag is checked for a PLUGINSPAGE attribute, and if one is found the PFS dialog will contain a "manual install" button that will load the PLUGINSPAGE url.

Omar Khan reported that if the PLUGINSPAGE attribute contains a javascript: url then pressing the button could launch arbitrary code capable of stealing local data or installing malicious code.

Element embed pluginspage attribute allows javascript urls, and somehow somebody forgot to sanitize it. So can execute arbitrary code.

Reproducible: Always

Steps to Reproduce:

1. Load page with an embed's pluginspage attribute set to javascript url
2. Click install missing plugins

3. Click Manual install Actual  
Results: Arbitrary code executed  
Expected Results: Do not execute arbitrary code.

**Solution**

Do security check when opening URL for manual plugin installation A cleaner way, without security manager checks would be:

```
nsPluginInstallerWizard.prototype.loadURL = function (aUrl){  
    if (window.opener.getBrowser().mCurrentBrowser)  
        window.opener.getBrowser().mCurrentBrowser.contentWindow.open(aUrl);  
}
```

use the current browser's contentWindow to open the url. This should be safe, thought perhaps if the current browser is pointing at an chrome:// url this could cause trouble. Probably needs more testing.

**Issue Tracking URL**

---

**Commit URL**

•

## CVE-2005-0590

**Context**

The underlying scenario is during an installation, in which the application displays a confirmation dialog that shows a spoofed URL.

**Problem**

Between not checking for a spoofed URL with a username/password, and the unresizable, unwrapped dialog for XPIInstall, it's possible to make a fairly convincing spoofed URL for an XPI with InstallTrigger, due to incorrect parsing of the URL.

**Solution**

The solution was to strip user:pass from URL display. It added a function that does a preprocessing of the URL (nsXPITriggerItem::GetSafeURLString()).

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=268059](https://bugzilla.mozilla.org/show_bug.cgi?id=268059)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=189142>
- <https://bugzilla.mozilla.org/attachment.cgi?id=174782>

## CVE-2005-0578

**Context**

Unsafe /tmp/plugtmp directory exploitable to erase user's files

**Problem**

A predictable name is used for the plugin temporary directory. A malicious local user could symlink this to the victim's home directory and wait for the victim to run Firefox. When Firefox shuts down the victim's directory would be erased. Mozilla creates the /tmp/plugtmp directory for storing plugin files, on exit, it empties this directory. A malicious local user could create a symlink at /tmp/plugtmp to a directory, when another user runs firefox the directory will be emptied. This is a serious issue on multiuser systems. Reproducible: Always Steps to Reproduce: 1. ln -s /home/taviso /tmp/plugtmp 2. wait for victim to run and exit firefox 3. victim just lost the files in his homedir. Actual Results: Example: \$ pwd /home/taviso \$ mkdir test \$ cd test \$ for ((i=0;<10;i++)); do touch \${RANDOM}.jpg; done \$ ls 10659.jpg 16835.jpg 26339.jpg 4062.jpg 8234.jpg 15120.jpg 22838.jpg 29316.jpg 724.jpg 9053.jpg # now malicious user wants to remove these files (i'll use user nobody for this example) \$ sudo -u nobody ln -s /home/taviso/test /tmp/plugtmp \$ ls -l /tmp/plugtmp lrwxrwxrwx 1 nobody nobody 17 Feb 6 18:43 /tmp/plugtmp -> /home/taviso/test/ # now malicious user waits until I run firefox... \$ firefox \$ ls \$ echo "arghhh, my files!" Expected Results: perhaps use a mkdtemp()-style directory instead of hardcoded /tmp/plugtmp?

**Solution**

Always create unique plugintmp directories for each browser instance, and only delete what was created.

**Issue Tracking URL**

---

**Commit URL**

•

## CVE-2005-0232

**Context**

Using Flash and the -moz-opacity filter you can get access to about:config and make the user silently change values

**Problem**

Plugins (such as flash) can be used to load privileged content into a frame. Once loaded, various spoofs can be applied to get the user to interact with the privileged content. Michael Krax's "Fireflashing" example demonstrates that an attacker can open about:config in a frame, hide it with an opacity setting, and if the attacker can get the victim to click at a particular spot (design some kind of simple game) you could toggle boolean preferences, some of which would make further attacks easier. The "firescrolling" example demonstrates arbitrary code execution (in this case downloading a file) by convincing the user to scroll twice. Details: Using Flash and the -moz-opacity filter it is possible to display the about:config site in a hidden frame. By making the user double-click at a specific screen position (e.g. using a DHTML game) you can toggle the status of boolean config parameters. As long as the number of about:config parameters is unchanged (unlikely a casual user will change them) you can move the parameter you want to change to the specified screen position by using CSS (change the .hideframe class). Reproducible: Always Steps to Reproduce: 1. Open <http://www.mikx.de/fireflashing/> 2. Open example link (make sure Flash 7 is installed) 3. Double click on the red box Actual Results: You can silently toggle any boolean config parameter Expected Results: Security manager should prevent that a plugin can open about:config or file:/// links

**Solution**

Do security checks when loading URLs from any plugin. This will enforce that plug-ins cannot open the about:config Webpage (that has access to privileges configuration) r=dveditz, but don't we need to do the same thing down in nsPluginHostImpl::PostURL ?

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=280664](https://bugzilla.mozilla.org/show_bug.cgi?id=280664)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=173316>

**CVE-2004-0762****Context**

During initialization of extensions

**Problem**

If a malicious Web site can control or predict when and where a user will click, it can get them to install software. Ways in which a Website can predict user clicks:

1. A game. 1a. Make the player "pick up" items by clicking them. Measure the speed with which the player moves the mouse and clicks, and once the speed stabilizes, pop up an install dialog just before the player clicks. 1b. Force the player to click at exactly the right time: a reaction-time test, shoot the monkey, etc. 1c. Convince the player to double-click an object whose location I control. 1d. Tell the player that he has infinite ammo and can shoot by pressing or holding the 'i' button on the keyboard. Pop up an install dialog when the player runs out of ammo.
2. Pop-up hell. 2a. Make the 'x' for the pop-up ad appear just where a security dialog will appear. 2b. Make fake pop-ups out of images so you can measure the victim's reaction time, average mouse acceleration, etc. Get them on the fifth "pop-up".

**Solution**

They enumerated three possible alternatives, and decided to implement the following:

B) Add a one-second delay between when the dialog gets focus and when the Install/OK button becomes enabled. I say "gets focus" rather than "appears" because a site could hide an install dialog as a modal dialog of a background window for a minute and then bring the dialog to the front at a convenient time by closing the window in front.

The other alternatives were (but they're not implemented):

A) When a site tries to install software or calls enablePrivilege, display a status bar message, "This page would like to install software on your computer". Only display the dialog after the user clicks the status bar message. (Err, how do you click a status bar message with the keyboard?) C) If the total time to decide to install and download the xpi are less than five seconds, stall installation (with the "downloading..." dialog still up) until five seconds are up so the user has an extra chance to cancel. I'm worried that users might not know to cancel because they do not realize that they accidentally clicked "install" in a dangerous dialog.

**Issue Tracking URL**

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=162020](https://bugzilla.mozilla.org/show_bug.cgi?id=162020)

**Commit URL**

- <https://bugzilla.mozilla.org/attachment.cgi?id=150067>

# OfBiz

## CVE-2017-15714

### Context

It occurs in the BIRT plug-in, in the code that is used to Map Java attributes to Javascript constants.

### Problem

The BIRT plugin in Apache OFBiz does not escape user input property passed. This allows for code injection by passing that code through the URL. For example by appending this code "`_format=%27;alert(%27xss%27)`" to the URL an alert window would execute.

### Solution

Fix is to enforce html encoding of request-strings passed to birt. This is done by invoking (which escapes HTML characters)

```
htmlEncode(ParameterAccessor.getFormat(request))
```

### Issue Tracking URL

- 

### Commit URL

- <https://svn.apache.org/viewvc?view=revision&revision=1818482>

# OpenMRS

## CVE-2017-12796

### Context

Deserialization of XML input into objects

### Problem

Exploitation of this vulnerability is possible through a single HTTP POST request to the page at `http://localhost/openmrs/admin/reports/reportSchemaXml.form`. Accessing this page through a browser without authenticating first will redirect the user to the login page (so far so good). Under the hood, however, the application is actually executing server-side code before the HTTP redirect response is generated (not so good). Through a Java debugger, with a few strategically placed breakpoints, it becomes apparent that a validation function is being called prior to any auth checks in the `reportSchemaXml` form controller. By itself, this is a relatively low-severity issue. The end result is still a HTTP 302 to the login page. The real problem here is revealed by stepping into the call to `reportService.getReportSchema(rsx)`. Within this function, a deserialization call can clearly be observed. Furthermore, this deserialization call takes as input user-provided data from the original POST request. Again, this is a pre-auth POST request; no authentication checks have been run. An additional step into the `deserialize()` function shows that XStream is being used for deserialization instead of builtin Java deserialization fuctions. At this point it has been established that the application is deserializing arbitrary input from an unauthenticated user without any filtering. For a full explanation of why this is so bad, and why this will almost certainly lead to some kind of RCE vulnerability, check out this article by FoxGlove Security. The next step in the exploitation process is to craft a malicious Java object that, when passed to the `XStream deserialize()` function, will result in RCE.

### Solution

Validation of the XML input before deserialization. This avoids that a plug-in injects OS commands.

### Issue Tracking URL

- <https://isears.github.io/jekyll/update/2017/10/21/openmrs-rce.html>

### Commit URL

---

# Pidgin

## CVE-2014-3694

### Context

Plug-ins: GnuTLS SSL/TLS and OpenSSL SSL/TLS plugin. It occurs during the handling of X.509 certificates from SSL servers.

### Problem

Both of libpurple's bundled SSL/TLS plugins (one for GnuTLS and one for NSS) failed to check that the Basic Constraints extension allowed intermediate certificates to act as CAs. This allowed anyone with any valid certificate to create a fake certificate for any arbitrary domain and Pidgin would trust it.

### Solution

Both bundled plugins were changed to check the Basic Constraints extension on all intermediate CA certificates.

### Issue Tracking URL

- <http://pidgin.im/news/security/?id=86>

### Commit URL

- <https://bitbucket.org/pidgin/main/commits/2e4475087f04>

## CVE-2013-6483

### Context

XMPP protocol plugin (when handling spoofed replies)

### Problem

The XMPP protocol plugin failed to ensure that iq (Instant Messaging Intelligence Quotient) replies came from the person they were sent to. A remote user could send a spoofed iq reply and attempt to guess the iq id. This could allow an attacker to inject fake data or trigger a null pointer dereference.

### Solution

Keep track of the 'to' when sending an iq stanza and make sure replies for a given stanza ID come from the same address it was sent to.

### Issue Tracking URL

- <http://pidgin.im/news/security/?id=78>

### Commit URL

- <https://bitbucket.org/pidgin/main/commits/93d4bff19574>

## CVE-2013-0271

### Context

MXit protocol plugin in libpurple (when handling invalid file paths)

### Problem

The MXit protocol plugin saves an image to local disk using a filename that could potentially be partially specified by the IM server or by a remote user, which could be used to create malicious files or overwrite files of the user.

### Solution

Escape values that come from the network before using them in filenames.

### Issue Tracking URL

- <http://www.pidgin.im/news/security/?id=65>

### Commit URL

- <https://bitbucket.org/pidgin/main/commits/a8ae1d340f2>

## CVE-2012-6152

### Context

Yahoo! protocol plugin in libpurple (during validation of incoming strings)

### Problem

Many places in the Yahoo! protocol plugin assumed incoming strings were UTF-8 and failed to transcode from non-UTF-8 encodings. This can lead to a crash when receiving strings that aren't UTF-8.

### Solution

Depending on the context, either validate that a string is UTF-8 or transcode the string from the appropriate encoding to UTF-8.

### Issue Tracking URL

- <http://pidgin.im/news/security/?id=70>

### Commit URL

- <https://bitbucket.org/pidgin/main/commits/b0345c25f886>

## CVE-2012-1178

### Context

A flaw was found in the way the Pidgin MSN protocol plug-in processed text that was not encoded in UTF-8. A remote attacker could use this flaw to crash Pidgin by sending a specially-crafted MSN message.

#### Problem

In some situations the MSN server sends text that isn't UTF-8 encoded, and Pidgin fails to verify the text's encoding. In some cases this can lead to a crash when attempting to display the text.

#### Solution

Verify that incoming text is UTF-8, and sanitize if it's not.

#### Issue Tracking URL

- <http://developer.pidgin.im/ticket/14884>
- <http://pidgin.im/news/security/?id=61>

#### Commit URL

- <https://bitbucket.org/pidgin/main/commits/5c02bc93f2c4>
- <https://bitbucket.org/pidgin/main/commits/85ec889f1675>
- <https://bitbucket.org/pidgin/main/commits/f9eeb175a5c9>
- <https://bitbucket.org/pidgin/main/commits/1b1b97b8e942>
- <https://bitbucket.org/pidgin/main/commits/f5fd49c83637>

## CVE-2011-4603

#### Context

SILC protocol plugin in libpurple during validation of incoming messages.

#### Problem

When receiving various incoming messages, the SILC protocol plugin failed to validate that a piece of text was UTF-8. In some cases invalid UTF-8 data would lead to a crash. This vulnerability is similar to CVE-2011-3594, but occurs in a different piece of code and was fixed at a later date.

#### Solution

Validate incoming strings as UTF-8 before using them as such.

#### Issue Tracking URL

- <http://www.pidgin.im/news/security/?id=59>

#### Commit URL

- <https://bitbucket.org/pidgin/main/commits/fa8d4132d071>

## CVE-2011-4601

#### Context

Oscar protocol plugin in libpurple during validation of incoming messages.

#### Problem

When receiving various messages related to requesting or receiving authorization for adding a buddy to a buddy list, the oscar protocol plugin failed to validate that a piece of text was UTF-8. In some cases invalid UTF-8 data would lead to a crash.

#### Solution

Validate incoming strings as UTF-8 before using them as such.

#### Issue Tracking URL

- <http://pidgin.im/news/security/?id=57>

#### Commit URL

- <https://bitbucket.org/pidgin/main/commits/8431da66063b>

## CVE-2011-3594

#### Context

SILC protocol plug-in when handling non-UTF8 strings using the glib2.

#### Problem

When receiving various incoming messages, the SILC protocol plugin failed to validate that a piece of text was UTF-8. In some cases invalid UTF-8 data would lead to a crash. A flaw was reported [1] in libpurple's SILC protocol plugin, and all software which uses SILC via libpurple. The `g_markup_escape_text()` function, when called on strings that have not been verified as valid UTF-8, will read past the end of the string and eventually `segfault` for certain sequences in some versions of Glib2. The behaviour of this function was undefined, and because it depends on the particular version of Glib2 in use, it is unknown what the complete ramifications of the flaw is, however it has been verified that an untrusted user could remotely crash a libpurple client via specially crafted SILC messages. The crash is caused by passing "user-controlled" non-UTF8 string to the `g_markup_escape_text` function. A non-utf8 string passed to `g_markup_escape_text` causes the same string to be passed along to `append_escaped_text` in `gmarkup.c` `append_escaped_text` is supposed to parse this text and uses `g_utf8_next_char` to read the entire input string (assuming that it is utf8 of course). `g_utf8_next_char` returns invalid pointers which causes "while (p != end)" loop in `append_escaped_text` to never exit. This ultimately causes OOB read and eventual client crash.

#### Solution

Validate incoming strings as UTF-8 before using them as such.

#### Issue Tracking URL

- <http://developer.pidgin.im/ticket/14636>
- <http://pidgin.im/news/security/?id=56>

#### Commit URL

- <https://bitbucket.org/pidgin/main/commits/69372ee4f474>

## CVE-2011-2943

### Context

IRC protocol plug-in when processing invalid nicknames

### Problem

A NULL pointer dereference flaw was found in the way IRC protocol plug-in of the Pidgin multiprotocol instant messaging client processed certain nick names, when list set of users (/who command) was issued upon user session startup and connecting user has had certain encoding configuration setup. A remote attacker could use a specially-crafted string as their nickname to cause the Pidgin client on the side of the victim (connecting user) to crash.

Certain characters in the nicknames of IRC users can trigger a null pointer dereference in the IRC protocol plugin's handling of responses to WHO requests. This can cause a crash on some operating systems. Clients based on libpurple 2.8.0 through 2.9.0 are affected.

### Solution

Change libpurple to validate the data it receives from the server before attempting to use it.

### Issue Tracking URL

- <http://pidgin.im/news/security/?id=53>

### Commit URL

- <https://bitbucket.org/pidgin/main/commits/619f32df41f1>

## CVE-2010-3088

### Context

Pidgin-knotify plug-in flaw when processing incoming messages

### Problem

pidgin-knotify is a pidgin plugin that displays received messages and other notices from pidgin as KDE notifications. It uses system() to invoke ktdialog and passes the unescaped messages as command line arguments. An attacker could use this to inject arbitrary commands by sending a prepared message via any protocol supported by pidgin to the victim.

*Reproducible:* Always

*Steps to Reproduce:*

1. Install and enable pidgin-knotify
2. Receive a message like ';touch /tmp/vulnerable;
3. Confirm that /tmp/vulnerable exists

*Actual Results:* /tmp/vulnerable exists

*Expected Results:* The touch command should not be run.

The vulnerable system() call is located in src/pidgin-knotify.c, line 71-74: command = g\_strdup\_printf("kdialog --title '%s' --passivepopup '%s' %d", title, body, timeout);  
[...] result = system(command);

### Solution

Instead of using system(), functions of the exec family should be used, e.g. execve with a sanitized environment. If a dbus interface for showing notifications in KDE exists, it could be used as well. I've written a patch some time ago to remove system() and instead use dbus, and upstream has given me access to the repository so I was planning to release a new version with that when RL shit happened and all my free time went to hell

### Issue Tracking URL

---

### Commit URL

---

## CVE-2010-0013

### Context

MSN protocol plugin in libpurple when processing emoticon messages

### Problem

Directory traversal vulnerability in slp.c in the MSN protocol plugin in libpurple in Pidgin 2.6.4 and Adium 1.3.8 allows remote attackers to read arbitrary files via a .. (dot dot) in an application/x-msnmsgrp2p MSN emoticon (aka custom smiley) request, a related issue to CVE-2004-0122.

*NOTE: it could be argued that this is resultant from a vulnerability in which an emoticon download request is processed even without a preceding text/x-mms-emoticon message that announced availability of the emoticon.*

### Solution

Remove ~/.purple/custom\_smiley/ directory if it exists. The directory is not created by default and is created when first custom smiley is defined.

### Issue Tracking URL

---

### Commit URL

---

# Thunderbird

## CVE-2016-1966

### Context

When Firefox handles NPAPI plug-ins that create multiple objects of type NPObj that needs to be wrapped with an Object Wrapper.

### Problem

We believe there to be an incorrect assumption regarding the purpose of a certain variable assignment which is assumed to be obsolete. The 'entry' variable is a pointer to an entry inside the data storage of the global 'sNPObjWrappers' (which keeps track of the object wrappers used in the application). This may cause the NPAPI subsystem to crash. The high-level PoC to trigger the vulnerability and cause a crash is as follows:  
1. write a NPAPI plug-in which has a function that creates and returns a new NPObj every time it is called; 2. call that function in a loop from Javascript. The browser will likely crash when a HashTable Object resizes its underlying data storage."

### Solution

Fix an erroneous nsNPObjWrapper assertion.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1246054](https://bugzilla.mozilla.org/show_bug.cgi?id=1246054)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=8716183>
- <https://bugzilla.mozilla.org/attachment.cgi?id=8720113>

## CVE-2013-1713

### Context

In the plugin extensions (when checking the principal when validating URI loads of extensions )

### Problem

The InstallTrigger component can use the wrong principal when validating URI loads. It was happening because this component was grabbing the origin information from the outer window. This is a potential concern in other javascript components that use the document of the window they're accessible from to perform checks against URLs before performing sensitive actions, and could also potentially be used to bypass the same origin policy and other all around nastiness.

### Solution

Fix is to get the principal information from the right context.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=887098](https://bugzilla.mozilla.org/show_bug.cgi?id=887098)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=768106>
- <https://bugzilla.mozilla.org/attachment.cgi?id=767910>

## CVE-2013-0747

### Context

Can confuse PluginHandler Event by listening for mutation events.

### Problem

JavaScript error: chrome://browser/content/browser.js, line 10437: iconStatus is null

```
>         let installStatus = doc.getAnonymousElementByAttribute(plugin, "class", "installStatus");
>         installStatus.setAttribute("status", "ready");
>         let iconStatus = doc.getAnonymousElementByAttribute(plugin, "class", "icon");
>         iconStatus.setAttribute("status", "ready");
```

The page gets an event whose originalTarget is an anonymous DIV. It is not expected that the page be able to get a reference to the anonymous content. • Content pages shouldn't be able to access native anon content. There used to be an exception if that happened. A dedicated attacker could turn it into something pretty serious by rearranging the anonymous DOM and clickjacking plugin install prompts.

### Solution

The fix was to add a <binding native="true"> attribute which would force the pluginProblem XBL subtree to be considered native-anonymous instead of just anonymous, which would prevent access from content script.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=733305](https://bugzilla.mozilla.org/show_bug.cgi?id=733305)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=662337>
- <https://bugzilla.mozilla.org/attachment.cgi?id=694813>

## CVE-2012-4194

### Context

Location can be spoofed using |valueOf|

### Problem

When Adobe Flash Player checks the page location to apply the SOP (Same-Origin Policy), it reads the return value of javascript:top.location+"\_\_flashplugin\_unique\_\_". When an object is joined with a string, its `|valueOf|` method is called before `|toString|`, and content can redefine the former. This appears to have regressed in Firefox v16.0.1.

In short, the property can be altered to gain access to attributes that are not supposed to be accessed.

#### Solution

Prevent shadow of built-in `location.valueOf`.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=800666](https://bugzilla.mozilla.org/show_bug.cgi?id=800666)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=674879>

## CVE-2012-3994

#### Context

Using `Object.defineProperty` to interfere with other add-ons (or the application).

#### Problem

The `Object.defineProperty` can shadow `|top|`. Plugins may try to access it through `|top.location|` -- for instance, Adobe Flash Player opens `javascript:top.location+"__flashplugin_unique__"` to determine the page origin. And it is possible to shadow `|top|` using `Object.defineProperty`. Incidentally, Google Chrome seems to disallow redefining `|top|`.

#### Solution

Reload Iframe and re-create docshell

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=765527](https://bugzilla.mozilla.org/show_bug.cgi?id=765527)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=650991>

## CVE-2012-3975

#### Context

The created document is a data document, so it itself shouldn't load anything. HTML parser may speculatively load something. (It shouldn't enable speculative loads for data documents)

#### Problem

This is a bad bug in the patch for bug 102699. Before that patch, the only codepath that could lead to parsing looked like this, in order: 1) Create a document with the DOMParser's `mOriginalPrincipal`. 2) Call `EnableXULXBL()` on the document if needed 3) Call `StartDocumentLoad()` 4) Set the document's base URI 5) Reset the document's principal to `mPrincipal`. 6) Feed data into the parser. That sequence of steps was pretty clearly documented (at least in terms of the whole principal dance) and `_very_critical`. When that bug was fixed, the XML codepath stayed as above, but HTML codepath was written more like this: 1) Create a document with the DOMParser's `mOriginalPrincipal`. 2) Feed data into the parser. 3) Call `EnableXULXBL()` on the document if needed 4) Set the document's base URI 5) Reset the document's principal to `mPrincipal`. But the whole point of resetting to `mPrincipal` is that it **MUST** happen before any data goes in. Otherwise you're parsing with the system principal. Also, this is never calling `StartDocumentLoad`, so afait it's not setting up whatever state that would normally set up (e.g. the document URI) the same way as the XML path. And it's calling `EnableXULXBL()` too late, of course. Not like this matters much for `text/html`. This bug means that using `DOMParser` on `text/html` is pretty unsafe from chrome: It allows whatever string you're parsing to poke any URI it wants, including ones that web content normally can't access. (On a Unix system it allows at minimum a DoS attack by reading from `file:///dev/tty`.)

#### Solution

make sure chrome `DOMParser` doesn't load external resources

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=770684](https://bugzilla.mozilla.org/show_bug.cgi?id=770684)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=640187>

## CVE-2012-3960

#### Context

During deallocation

#### Problem

Use-after-free vulnerability in `mozSpellChecker::SetCurrentDictionary`. `mozSpellChecker::SetCurrentDictionary` gets called, and then `mozHunspell::SetDictionary` gets called (which is inlined), which in turn calls into the notification service: . The editor then catches that notification and calls `nsEditor::SyncRealTimeSpell`, which can potentially lead into `moInlineSpellChecker` to get set to null , which in turn releases its `mSpellChecker` member , which is a `mozSpellChecker` which we see on the 1st frame of the freeing call stack. Then, all of this stuff returns, and when we get back to the `mozSpellChecker::SetCurrentDictionary` frame, \*this is dead, so any attempt to call it (such as calling `Release` on it) will dereference freed memory. Now, I \_think\_ that you can't put arbitrary stuff on the stack between the time that the `mozSpellChecker` object dies and the time that `mozSpellChecker::SetCurrentDictionary` returns, but if I'm wrong, and you could do that, then this gives you a very nice remote exploit, because the offset of `Release` in the vtable is pretty well known...

#### Solution

Part 1: Make sure that `mozSpellChecker`'s refcount doesn't go down prematurely; Part 2: Make sure that `nsEditorSpellCheck`'s refcount doesn't go down prematurely;  
Part 3: Make sure that `nsEditorSpellCheck`'s refcount doesn't go down prematurely;

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=771976](https://bugzilla.mozilla.org/show_bug.cgi?id=771976)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=641142>
- <https://bugzilla.mozilla.org/attachment.cgi?id=642856>

- <https://bugzilla.mozilla.org/attachment.cgi?id=643240>

## CVE-2012-1956

### Context

It occurs when extensions manipulate the Object.defineProperty as a method to shadow the location object (aka window.location)

### Problem

It is possible to shadow the location object using Object.defineProperty. This could be used to confuse the current location to plugins, allowing for possible cross-site scripting (XSS) attacks. It means that an attacker can confuse Flash (or other plugins) into thinking that we're on one domain when, in reality, we're on another one leading to XSS attacks.

### Solution

Create a function that does security checks specifically for the object (js::CheckDefineProperty(JSContext \*cx, HandleObject obj, HandleId id, HandleValue value, PropertyOp getter, StrictPropertyOp setter, unsigned attrs)).

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=756719](https://bugzilla.mozilla.org/show_bug.cgi?id=756719)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=667903>
- <https://bugzilla.mozilla.org/attachment.cgi?id=634237>

## CVE-2012-0446

### Context

It occurs when frame scripts that call untrusted objects.

### Problem

Frame scripts bypass XPConnect security checks when calling untrusted objects. This allows for cross-site scripting (XSS) attacks through web pages and Firefox extensions. Frame scripts run on the special JS context for which we call SetSecurityManagerForJSContext with flags=0, thus if a frame script calls into an untrusted function, XPConnect does not do proper security checks.

### Solution

The fix enables the Script Security Manager (SSM) to force security checks on all frame scripts.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=705651](https://bugzilla.mozilla.org/show_bug.cgi?id=705651)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=577960>
- <https://bugzilla.mozilla.org/attachment.cgi?id=577535>
- <https://bugzilla.mozilla.org/attachment.cgi?id=578220>

## CVE-2011-3001

### Context

It occurs as part of a user-assisted attack. If you could convince a user to hold down the Enter key--as part of a game or test, perhaps--a malicious page could pop up a download dialog where the held key would then activate the default Open action.

### Problem

For some file types this would be merely annoying (the equivalent of a pop-up) but other file types have powerful scripting capabilities. And this would provide an avenue for an attacker to exploit a vulnerability in applications not normally exposed to potentially hostile internet content. There are 2 layers of protection against an unauthorized installation of extensions: 1) The principal of the opener is checked against whitelisted domains that are allowed to download the plugin without asking. If the domain is not trusted, the user is asked to allow to download the plugin. 2) When the plugin is downloaded, the user is asked to confirm the installation. The first protection can be circumvented by creating a hidden "Embed" element containing an arbitrary XPI as its "pluginspage" parameter. The attacker can focus this element while the user holds Enter, causing a number of "Plugin Finder Service" windows to appear. The first window focuses the "Cancel" button and will just close, but all the subsequent ones will set focus on the "Manual Install" button directing to the malicious XPI. As soon as the user releases the key, the browser will start launching multiple windows with the provided URL. The windows will have a ChromeWindow object as their opener, so the user will not be asked to allow to download a plugin. The second protection can be bypassed due to a logic error in amWebInstallListener.js. When no window-watcher is registered in Services, this will throw:

### Solution

It ensures that window watcher is defined, such that it can show the install dialog.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=672485](https://bugzilla.mozilla.org/show_bug.cgi?id=672485)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=555021>

## CVE-2010-1585

### Context

During Plug-ins execution (protection mechanism against unsafe javascript).

### Problem

The two ns(X)HTMLParanoidFragmentSink classes are used by nsIScriptableUnescapeHTML to sanitize (X)HTML by stripping attributes and tags not on a built-in whitelist. It allows javascript: URLs and other inline JavaScript when the embedding document is a chrome document. While there are no unsafe uses of this class in any released products, extension code could have potentially used it in an unsafe manner. The sinks attempt to sanitize URLs by calling

CheckLoadURI[...]DISALLOW\_INHERIT\_PRINCIPAL), but unfortunately when the target document is a chrome document (as is common with add-ons) this check allows any URI. In particular malicious href="javascript:evil()" or <iframe src="data:evil"> can slip through and create sg-critical bugs.  
In short, it 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.

#### Solution

DISALLOW\_INHERIT\_PRINCIPAL always returned "ok" for system principals. Therefore, they used a null principal when performing the validation.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=562547](https://bugzilla.mozilla.org/show_bug.cgi?id=562547)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=442465>
- <https://bugzilla.mozilla.org/attachment.cgi?id=497538>
- <https://bugzilla.mozilla.org/attachment.cgi?id=497566>
- <https://bugzilla.mozilla.org/attachment.cgi?id=499199>

## CVE-2010-0179

#### Context

When dispatching events from the XMLHttpRequestSpy module (a Firebug add-on)

#### Problem

When accessing this.xhrRequest.onreadystatechange, content functions (QueryInterface, getInterfaces, etc.) can be called. In other words, when add-ons try to get a reference to onreadystatechange, we call getInterfaces on the existing handler (through the nsXPCWrappedJS). Since the application does not properly handle interaction between the XMLHttpRequestSpy object and chrome privileged objects, it allows remote attackers to execute arbitrary JavaScript via a crafted HTTP response.  
In short: Add-ons can get more information from calling functions they're not supposed to because the application doesn't check for the principal.

#### Solution

The fix is to check the correct principal (origin). "If no scripted code is running "above" (or called from) fp, then instead of looking at cx->globalObject, |principal| is returned."

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=504021](https://bugzilla.mozilla.org/show_bug.cgi?id=504021)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=395462>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410791>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410788>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410808>
- <https://bugzilla.mozilla.org/attachment.cgi?id=410809>
- <https://bugzilla.mozilla.org/attachment.cgi?id=423691>
- <https://bugzilla.mozilla.org/attachment.cgi?id=425570>

## CVE-2008-2806

#### Context

Mozilla.org distributions on the Mac that can use Java have for some time bundled the Java Embedding Plugin, which allows non-WebKit browsers to use current Java versions on OS X.

#### Problem

The Firefox Mac OS X Java Plugin (MRJ Plugin) is vulnerable to the 'document.domain' bypass. Document.domain gets/sets the domain portion of the origin of the current document, as used by the same origin policy. By using the document.domain exception to the same origin policy, LiveConnect, which is a feature of web browsers which allows Java applets to communicate with the JavaScript engine in the browser, and JavaScript on the web page to interact with applets, can be used to create arbitrary socket connections. The code appears to use nsIPrincipal::GetOrigin(), an interface to a principal, which represents a security context, which takes document.domain into account.

In short, the issue was with how the plugin for Java applets makes calls to javascript and obtains the origin of the domains, bypassing the same origin policy.

#### Solution

The fix was to drop any use of GetOrigin() for Java and use the principal's URI

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=408329](https://bugzilla.mozilla.org/show_bug.cgi?id=408329)

#### Commit URL

---

## CVE-2008-2803

#### Context

When loading scripts from extensions (function: mozIJSSubScriptLoader.LoadScript )

#### Problem

It's unsafe to use mozIJSSubScriptLoader.loadSubScript() with non-chrome urls or chrome urls whose scheme/host part contain uppercase characters. Scripts that are loaded in this way do not use implicit XPCNativeWrappers when accessing content, which is used whenever privileged code is used to access unprivileged code. It is used to create a security wrapper that guarantees that the "native" methods/properties of an object will be called (and not the methods overridden by the webpage). As an example, Google Toolbar uses mozIJSSubScriptLoader.loadSubScript() with file: url, and allows an attacker to run arbitrary code with chrome privileges.

#### Solution

They fixed their logic for obtaining a native object wrapper. The decision of whether the subscript gets XPCNativeWrappers or not will depend on the caller, not the file:// URI.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=418356](https://bugzilla.mozilla.org/show_bug.cgi?id=418356)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=310920>
- <https://bugzilla.mozilla.org/attachment.cgi?id=323747>
- <https://bugzilla.mozilla.org/attachment.cgi?id=310145>

## CVE-2007-3844

#### Context

When handling Privileges of plug-ins

#### Problem

window.open("about:blank"); or content.location = "about:blank"; or about:blank when loaded by chrome in these ways has chrome privileges. This behavior could cause security issues in certain extensions that are thinking that about:blank does not have chrome privileges. Imagine an extension that does: 1. Collect urls from content. 2. Load about:blank. (window.open("about:blank") or content.location = "about:blank") 3. Generate links with the urls and insert those into the about:blank document. When an user clicks a javascript: link in the generated page, the script run with chrome privileges. I'm not sure whether this should be fixed or not. If not, we need to advertise the potential problem. (There is an affected extension on AMO.)

#### Solution

The three hunks of this patch do the following: 1) Never allow chrome-privileged data:, javascript:, or about:blank loads in content docshells. Switch them to inheriting principals instead (which is a no-op for about:blank). This behavior is now consistent across all "normal" ways of loading, whereas before window.location allowed chrome javascript: while the nsIWebNavigation APIs, tabbrowser, and setting "src" on s did not. It's still possible to do such loads via manual invocation of nsILinkHandler, but that's not a scriptable API, and doesn't take a principal pointer anyway (it takes a node). This fixes the window.location aspect of this bug. 2) Don't propagate a system principal as the opener principal to new content windows. This fixes the window.open() aspect of this bug. Note that we need both, because CreateAboutBlankContentViewer doesn't actually do a load. 3) Remove now-redundant code in nsFrameLoader. The only risk here, imo is that this does change the behavior of data: and javascript: URIs loaded from chrome in content windows via window.location. If we want I can try to avoid changing that, but the code would be more complex, and I don't think we want to allow it anyway. The former is certainly not safe.

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=388121](https://bugzilla.mozilla.org/show_bug.cgi?id=388121)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=272411>
- <https://bugzilla.mozilla.org/attachment.cgi?id=272432>

## CVE-2006-6499

#### Context

The problem is in the JavaScript Engine ( function: jsdtoa)

#### Problem

When a plugin decreases the float precision (a global configuration) it triggers a bug in the javascript engine. In short, a loop in this engine is controlled by the floating point arithmetic. Since that is flawed (or rather becomes flawed after the precision is reduced), the loop becomes infinite, and it keeps adding characters to the string until it crashes. Detailed report: Crash in jsdtoa after opening a new window. There is some very bad logic in jsdtoa, for the case where the double has no fractional component. File: jsdtoa.c See line 2376 /\* Do we have a "small" integer? \*/ In that case there is a loop that converts the double to a string, one digit at a time. In the loop, it looks at the most significant digit, adds that digit to the string, and then removes the digit from the double value. Then, it multiples the value by 10 so shift the digits over to the left. The problem is that the looping logic is dependent on no floating point error being introduced. But, floating point error is introduced when two doubles of different magnitudes are subtracted, which is done here: 2388: d -= L\*ds; The check to exit the loop looks like this: 2410: if (!|d| >= 10.) break; It compares the double value to zero. Unfortunately, there is floating point error introduced, and the value of "d" never gets down to zero. Therefore, the loop becomes infinite, and we keep appending characters to the output string, ignoring the specified size of the buffer. (The buffer size test was done previously, based on the number of digits that it planned to place in the buffer). My proposed fix is rather simple. Since we know up front how many digits we have to write out, we can use that number to specify the number of times that we loop, rather than depending on errorless floating point math. See the diff between the original and modified files attached. I changed the "for" line: From: for(i = 1; ; i++) { To: for(i = 1; i <= k+1; i++) { And, I removed the check on the bottom of the for loop. From: if (!|d| >= 10.) break; To: d \*= 10.; Furthermore, the logic that is there is very bad. [Description about other problem cut, will file another bug where necessary.]

#### Solution

They fixed the calculations in the loop. [SIDE NOTE] Even though the bug looks like a simple error logic in a loop, from what I saw in the discussions, if they had used the Chrome's approach of isolating javascript objects, this bug would never be exploited. Why? In Chrome, Javascript objects are different (each plugin has its own JS objects), this means that plugins cannot interfere with each other nor the hosting application. Thus, even if a plug-in had decreased the floating precision, the crash would not occur. So the problem seems more like not properly isolating JS objects between plugins and Thunderbird

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=358569](https://bugzilla.mozilla.org/show_bug.cgi?id=358569)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=245115>

## CVE-2005-0590

#### Context

The underlying scenario is during an installation, in which the application displays a confirmation dialog that shows a spoofed URL.

#### Problem

Between not checking for a spoofed URL with a username/password, and the unresizable, unwrapped dialog for XPIInstall, it's possible to make a fairly convincing spoofed URL for an XPI with InstallTrigger, due to incorrect parsing of the URL.

#### Solution

The solution was to strip user:pass from URL display. It added a function that does a preprocessing of the URL (nsXPITriggerItem::GetSafeURLString()).

#### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=268059](https://bugzilla.mozilla.org/show_bug.cgi?id=268059)

#### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=189142>
- <https://bugzilla.mozilla.org/attachment.cgi?id=174782>

## CVE-2004-0906

### Context

It happened at the XPIInstall Engine

### Problem

After installation, many installed files are GROUP and WORLD writable, even though the installer was executed with the umask value 0022. In details: When files are installed via XPIInstall, the user's umask is ignored. The XPIInstall engine should respect the user's umask setting. The problem code is here: nsZipArchive::ExtractFile http://lxr.mozilla.org/mozilla/source/modules/libjar/nsZipArchive.cpp#641 nsJAR::Extract http://lxr.mozilla.org/mozilla/source/modules/libjar/nsJAR.cpp#251 both open the file with 0644 perms and then chmod the file to the appropriate perms, but this sidesteps any umask. Just to make things more complicated, the nsZipArchive is part of standalone libjar, where PR\_Open is defined as fopen in zipstub.h, so passing the file's mode to PR\_Open wouldn't work in that situation.

In short, the extraction of extensions files was made with wrong file permissions, creating world-readable/writeable files. This allows a trojan to modify a benign application for malicious purposes.

### Solution

The fix was setting the permissions on the extraction function.

### Issue Tracking URL

[https://bugzilla.mozilla.org/buglist.cgi?bug\\_id=235781,231083](https://bugzilla.mozilla.org/buglist.cgi?bug_id=235781,231083)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=155103>
- <https://bugzilla.mozilla.org/attachment.cgi?id=142413>
- <https://bugzilla.mozilla.org/attachment.cgi?id=142369>

## CVE-2004-0762

### Context

During initialization of extensions

### Problem

If a malicious Web site can control or predict when and where a user will click, it can get them to install software. Ways in which a Website can predict user clicks:

1. A game. 1a. Make the player "pick up" items by clicking them. Measure the speed with which the player moves the mouse and clicks, and once the speed stabilizes, pop up an install dialog just before the player clicks. 1b. Force the player to click at exactly the right time: a reaction-time test, shoot the monkey, etc. 1c. Convince the player to double-click an object whose location I control. 1d. Tell the player that he has infinite ammo and can shoot by pressing or holding the 'i' button on the keyboard. Pop up an install dialog when the player runs out of ammo.
2. Pop-up hell. 2a. Make the 'x' for the pop-up ad appear just where a security dialog will appear. 2b. Make fake pop-ups out of images so you can measure the victim's reaction time, average mouse acceleration, etc. Get them on the fifth "pop-up".

### Solution

They enumerated three possible alternatives, and decided to implement the following:

B) Add a one-second delay between when the dialog gets focus and when the Install/OK button becomes enabled. I say "gets focus" rather than "appears" because a site could hide an install dialog as a modal dialog of a background window for a minute and then bring the dialog to the front at a convenient time by closing the window in front.

The other alternatives were (but they're not implemented):

A) When a site tries to install software or calls enablePrivilege, display a status bar message, "This page would like to install software on your computer". Only display the dialog after the user clicks the status bar message. (Err, how do you click a status bar message with the keyboard?) C) If the total time to decide to install and download the xpi are less than five seconds, stall installation (with the "downloading..." dialog still up) until five seconds are up so the user has an extra chance to cancel. I'm worried that users might not know to cancel because they do not realize that they accidentally clicked "install" in a dangerous dialog.

### Issue Tracking URL

- [https://bugzilla.mozilla.org/show\\_bug.cgi?id=162020](https://bugzilla.mozilla.org/show_bug.cgi?id=162020)

### Commit URL

- <https://bugzilla.mozilla.org/attachment.cgi?id=150067>

# WordPress

## CVE-2013-7279

### Context

Cross-site scripting (XSS) vulnerability in views/video-management/preview\_video.php in the S3 Video plugin before 0.983 for WordPress allows remote attackers to inject arbitrary web script or HTML via the base parameter.

### Problem

S3 Video plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the preview\_video.php script. A remote attacker could exploit this vulnerability using the base parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

### Solution

Fixed security issue and tested with Wordpress 3.8 Fixed XSS scripting vulnerability in video preview script

### Issue Tracking URL

---

### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fs3-video&old=823847&new\\_path=%2Fs3-video&new=823847](http://plugins.trac.wordpress.org/changeset?old_path=%2Fs3-video&old=823847&new_path=%2Fs3-video&new=823847)

## CVE-2013-5963

### Context

WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in wp-content/uploads/wpdb/.

### Problem

#1.run the Firefox browser #2.Then Add-ons Live HTTP headers in Firefox Install >> #https://addons.mozilla.org/en-us/firefox/addon/live-http-headers/ #3.Now the run Add-ons Live HTTP headers #4.Then go to this page site/[path]/wp-content/plugins/simple-dropbox-upload-form/multi.php?&height=500&width=1000&TB\_iframe=true #5.Click the Choose File button Then select a file [shell.jpg] #6.Then click on the Start upload button #7.Now using Live HTTP headers uploaded files to PHP change [shell.php] #8.Find your Shell site/wp-content/uploads/wpdb/shell.php

### Solution

Removed multi.php

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset?reponame=&old=774214@simple-dropbox-upload-form%2Ftrunk&new=774214@simple-dropbox-upload-form%2Ftrunk>

## CVE-2013-5098

### Context

Download Monitor 'sort' Parameter Cross Site Scripting Vulnerability

### Problem

The Download Monitor plugin for WordPress is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

### Solution

Sanitized the sort parameter, by invoking the function sanitize\_text\_field()

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset/723187/download-monitor>

## CVE-2013-4954

### Context

WordPress Pie Register Plugin 'wp-login.php' Multiple Cross Site Scripting Vulnerabilities

### Problem

Pie Register plugin for WordPress is prone to multiple cross-site scripting vulnerabilities. An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and launch other attacks. Input is not sanitized before being output on the screen:

```
<?php echo $_POST['pass1'];?>
<?php echo $_POST['pass2'];?>
```

### Solution

Escaping of HTML/Javascript using html\_entity\_decode:

```
<?php echo htmlspecialchars($_POST['pass1']);?> <?php echo htmlspecialchars($_POST['pass2']);?>
```

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset?reponame=&old=740249%40pie-register&new=740249%40pie-register>

## CVE-2013-3532

### Context

WordPress Spider Video Player Plugin 'theme' Parameter SQL Injection Vulnerability

### Problem

Spider Video Player plugin for WordPress is prone to an SQL-injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Video Player Plugin for WordPress is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements to the settings.php script using the playlist and theme parameters, which could allow the attacker to view, add, modify or delete information in the back-end database.

### Solution

Sanitize input

### Issue Tracking URL

---

### Commit URL

---

## CVE-2013-3529

### Context

WordPress FuneralPress Plugin Multiple HTML Injection Vulnerabilities

### Problem

The FuneralPress plugin for WordPress is prone to multiple HTML-injection vulnerabilities because it fails to properly sanitize user-supplied input. Attacker-supplied HTML and script code would run in the context of the affected browser, potentially allowing the attacker to or control how the site is rendered to the user. Other attacks are also possible.

### Solution

sanitize text fields

### Issue Tracking URL

---

### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fwp-funeral-press&old=690038&new\\_path=%2Fwp-funeral-press&new=690038](http://plugins.trac.wordpress.org/changeset?old_path=%2Fwp-funeral-press&old=690038&new_path=%2Fwp-funeral-press&new=690038)

## CVE-2013-3526

### Context

WordPress Traffic Analyzer Plugin 'aoid' Parameter Cross Site Scripting Vulnerability

### Problem

The Traffic Analyzer plugin for WordPress is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.

### Solution

sanitize input

### Issue Tracking URL

---

### Commit URL

---

## CVE-2013-3491

### Context

WordPress Sharebar Plugin CVE-2013-3491 Cross Site Request Forgery Vulnerability

### Problem

The Sharebar plugin for WordPress is prone to a cross-site request-forgery vulnerability. Exploiting this issue may allow a remote attacker to perform certain unauthorized actions in the context of the affected application. Other attacks are also possible.

### Solution

sanitize input

### Issue Tracking URL

---

### Commit URL

---

## CVE-2013-3262

### Context

Download Monitor 'p' Parameter Cross Site Scripting Vulnerability

### Problem

The Download Monitor plugin for WordPress is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

**Solution**

Description: Note: This plugin is no longer actively developed nor maintained! However, a rewrite is planned - <http://mikejolley.com/2013/04/the-new-download-monitor-plugin/> Manage downloads on your site, view and show hits, and output in posts. sanitize\_text\_field to prevent XSS in admin

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/723187/download-monitor>

## CVE-2013-3253

**Context**

WordPress Xhanch - My Twitter Plugin CVE-2013-3253 Cross Site Request Forgery Vulnerability

**Problem**

The Xhanch - My Twitter plugin for WordPress is prone to a cross-site request-forgery vulnerability. Exploiting this issue may allow a remote attacker to perform certain unauthorized actions in the context of the affected application. Other attacks are also possible.

**Solution**

Security n hashtag

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/750054/xhanch-my-twitter>

## CVE-2013-2741

**Context**

The final step in the importbuddy backup restoration process is supposed to remove importbuddy.php from the root of the site, however this step often fails (most commonly as a result of filesystem permissions) allowing an attacker access to some or all of the functions and information provided by importbuddy.php. An access password for importbuddy does not appear to be a mandatory requirement.

**Problem**

The name of the backup file contains a random string intended to prevent an attacker from guessing its value. However if backup files are present, browsing to <http://site/importbuddy.php> will expose their filenames; these can then be used to download the files from the site: [backup-zipfile-date-randomstring.zip](http://site/backup-zipfile-date-randomstring.zip) The backup file can be retrieved with: wget <http://site/backup-zipfile-date-randomstring.zip> The backup consists of a zip archive containing the wordpress directory, complete with wp-config.php and often a .sql dump containing a full copy of the wordpress database and any other databases the backupbuddy plugin has been configured to include. Importbuddy also presents the option to upload a backup on step 1 of the restoration process, potentially allowing defacement or deletion and also trojaning the site if an existing backup is available. Additionally there are issues affecting the 'step' query string field. This has a differing impact depending on the version of Backupbuddy targeted: <http://site/importbuddy.php?step=1>

**Solution**

Forcing the user to set a password (and fixing the authentication bypass) would go some way to mitigating the risk of importbuddy.php not being deleted.

**Issue Tracking URL**

---

**Commit URL**

---

## CVE-2013-2640

**Context**

WordPress does not properly restrict access to unspecified Ajax functions, which allows remote attackers to modify plugin settings and conduct cross-site scripting (XSS) attacks via unspecified vectors related to "formData=save" requests

**Problem**

WordPress does not properly restrict access to unspecified Ajax functions, which allows remote attackers to modify plugin settings and conduct cross-site scripting (XSS) attacks via unspecified vectors related to "formData=save" requests

**Solution**

Security vulnerability has been patched with `is_user_logged_in()` and now submitted to first review

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?new=682420>

## CVE-2013-2501

**Context**

WordPress Terillion Reviews Plugin Profile Id HTML Injection Vulnerability

**Problem**

The Terillion Reviews plugin for WordPress is prone to an HTML-injection vulnerability because it fails to properly sanitize user-supplied input before using it in dynamically generated content. Successful exploits will allow attacker-supplied HTML and script code to run in the context of the affected browser, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible.

**Solution**

Fix security vulnerability by sanitizing user input

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/683838/terillion-reviews>

**CVE-2013-2204****Context**

Content Spoofing in the MoxieCode (TinyMCE) MoxiePlayer project

**Problem**

Flash doesn't recognize '#' symbol as the beginning of the fragment to ignore, so if '?' mark follows, remaining part of the url will still be interpreted as application parameters...

**Solution**

Consider part of url after '?' as querystring, no matter what precedes it.

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2013-1464****Context**

WordPress Audio Player SWF Cross Site Scripting

**Problem**

WordPress Audio Player Plugin 'playerID' Parameter Cross Site Scripting Vulnerability The Audio Player plugin for WordPress is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.

**Solution**

sanitize input

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2013-1409****Context**

Cross-Site Scripting (XSS) in CommentLuv wordpress plugin

**Problem**

The vulnerability exists due to insufficient filtration of user-supplied data in "\_ajax\_nonce" HTTP POST parameter in the "/wp-admin/admin-ajax.php" script. A remote attacker can trick a logged-in administrator to open a specially crafted link and execute arbitrary HTML and script code in browser in context of the vulnerable website. PoC (Proof-of-Concept) below uses the "alert()" JavaScript function to display administrator's cookies

**Solution**

Upgrade to CommentLuv 2.92.4

filter user supplied data

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2013-0735****Context**

WordPress Mingle Forum Plugin Multiple SQL Injection and Cross Site Scripting Vulnerabilities

**Problem**

The Mingle Forum plug-in for WordPress is prone to multiple SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user-supplied input. Exploiting these vulnerabilities could allow an attacker to steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

**Solution**

sanitize user-supplied data

**Issue Tracking URL**

---

**Commit URL**

---

## CVE-2013-0734

### Context

WordPress Mingle Forum Plugin Multiple SQL Injection and Cross Site Scripting Vulnerabilities

### Problem

The Mingle Forum plug-in for WordPress is prone to multiple SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user-supplied input. Exploiting these vulnerabilities could allow an attacker to steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

### Solution

sanitize user-supplied data

### Issue Tracking URL

---

### Commit URL

---

## CVE-2013-0731

### Context

WordPress MailUp Plugin Security Bypass Vulnerability

### Problem

WordPress does not properly restrict access to unspecified Ajax functions, which allows remote attackers to modify plugin settings and conduct cross-site scripting (XSS) attacks by setting the `wordpress_logged_in` cookie.

### Solution

Security vulnerability has been patched with `is_user_logged_in()` and now submitted to first review

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset?new=682420>

## CVE-2012-6527

### Context

Cross-site scripting (XSS) vulnerability in the My Calendar plugin before 1.10.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the `PATH_INFO`.

### Problem

My Calendar plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

### Solution

escape urls before use. Confirm that event ids are integers.

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset/490070/my-calendar>

## CVE-2012-5328

### Context

Multiple SQL injection vulnerabilities in the Mingle Forum plugin 1.0.32.1 and other versions before 1.0.33 for WordPress might allow remote authenticated users to execute arbitrary SQL commands via the (1) `memberid` or (2) `groupid` parameters in a `removemember` action or (3) `id` parameter to `fs-admin/fs-admin.php`, or (4) `edit_forum_id` parameter in an `edit_save_forum` action to `fs-admin/wpf-edit-forum-group.php`.

### Problem

Sql injection vulnerabilities.

### Solution

escape data in post request before performing sql operations.

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=492859@mingle-forum&old=487353@mingle-forum>

## CVE-2012-5327

### Context

Multiple SQL injection vulnerabilities in `fs-admin/fs-admin.php` in the Mingle Forum plugin 1.0.32.1 and other versions before 1.0.33 for WordPress allow remote authenticated users to execute arbitrary SQL commands via the (1) `delete_usgrp[]` parameter in a `delete_usergroups` action, (2) `usergroup` parameter in an `add_user_togroup` action, or (3) `add_forum_group_id` parameter in an `add_forum_submit` action.

### Problem

WordPress Mingle Forum Plugin is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements to the admin.php script using the multiple parameters, which could allow the attacker to view, add, modify or delete information in the back-end database.

**Solution**

escape data in post requests before doing database operations.

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=492859@mingle-forum&old=487353@mingle-forum>

## CVE-2012-4283

**Context**

Cross-site scripting (XSS) vulnerability in the Login With Ajax plugin before 3.0.4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the callback parameter.

**Problem**

XSS in Login with Ajax plugin

**Solution**

use regex to match the expected query string

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/541069>

## CVE-2012-4273

**Context**

Cross-site scripting (XSS) vulnerability in libs/xing.php in the 2 Click Social Media Buttons plugin before 0.34 for WordPress allows remote attackers to inject arbitrary web script or HTML via the xing-url parameter.

**Problem**

2 Click Social Media Buttons plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the xing.php script. A remote attacker could exploit this vulnerability using the xing-url parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

**Solution**

strip tags from url

**Issue Tracking URL**

---

**Commit URL**

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2F2-click-socialmedia-buttons&old=532798&new\\_path=%2F2-click-socialmedia-buttons&new=532798](http://plugins.trac.wordpress.org/changeset?old_path=%2F2-click-socialmedia-buttons&old=532798&new_path=%2F2-click-socialmedia-buttons&new=532798)

## CVE-2012-4272

**Context**

Multiple cross-site scripting (XSS) vulnerabilities in the 2 Click Social Media Buttons plugin before 0.34 for WordPress allow remote attackers to inject arbitrary web script or HTML via unspecified vectors related to the "processing of the buttons of Xing and Pinterest".

**Problem**

XSS vulnerabilities in Click Social Media Buttons plugin

**Solution**

strip tags before decoding raw url

**Issue Tracking URL**

---

**Commit URL**

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2F2-click-socialmedia-buttons&old=532798&new\\_path=%2F2-click-socialmedia-buttons&new=532798](http://plugins.trac.wordpress.org/changeset?old_path=%2F2-click-socialmedia-buttons&old=532798&new_path=%2F2-click-socialmedia-buttons&new=532798)

## CVE-2012-4271

**Context**

Multiple cross-site scripting (XSS) vulnerabilities in bad-behavior-wordpress-admin.php in the Bad Behavior plugin before 2.0.47 and 2.2.x before 2.2.5 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) PATH\_INFO, (2) httpbl\_key, (3) httpbl\_maxage, (4) httpbl\_threat, (5) reverse\_proxy\_addresses, or (6) reverse\_proxy\_header parameter.

**Problem**

Bad Behavior plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the options-general.php script. A remote attacker could exploit this vulnerability using multiple parameters in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

**Solution**

escape url before use (sanitize)

**Issue Tracking URL**

---

**Commit URL**

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fbad-behavior&old=543807&new\\_path=%2Fbad-behavior&new=543807](http://plugins.trac.wordpress.org/changeset?old_path=%2Fbad-behavior&old=543807&new_path=%2Fbad-behavior&new=543807)

## CVE-2012-4268

### Context

Cross-site scripting (XSS) vulnerability in bulletproof-security/admin/options.php in the BulletProof Security plugin before .47.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the HTTP\_ACCEPT\_ENCODING header.

### Problem

BulletProof Security plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the admin.php script. A remote attacker could exploit this vulnerability using the page parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

### Solution

filter and sanitize input string before use.

### Issue Tracking URL

---

### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fbulletproof-security&old=543044&new\\_path=%2Fbulletproof-security&new=543044](http://plugins.trac.wordpress.org/changeset?old_path=%2Fbulletproof-security&old=543044&new_path=%2Fbulletproof-security&new=543044)

## CVE-2012-4264

### Context

Multiple cross-site scripting (XSS) vulnerabilities in the Better WP Security (better\_wp\_security) plugin before 3.2.5 for WordPress allow remote attackers to inject arbitrary web script or HTML via unspecified vectors related to "server variables," a different vulnerability than CVE-2012-4263.

### Problem

XSS vulnerabilities in Better WP Security plugin

### Solution

filter and sanitize string before use.

### Issue Tracking URL

---

### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fbetter-wp-security&old=542852&new\\_path=%2Fbetter-wp-security&new=542852](http://plugins.trac.wordpress.org/changeset?old_path=%2Fbetter-wp-security&old=542852&new_path=%2Fbetter-wp-security&new=542852)

## CVE-2012-4263

### Context

Cross-site scripting (XSS) vulnerability in inc/admin/content.php in the Better WP Security (better\_wp\_security) plugin before 3.2.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the HTTP\_USER\_AGENT header.

### Problem

The value of the User-Agent HTTP header is copied into the HTML document as plain text between tags. The payload a712378089b4648b was submitted in the User-Agent HTTP header. This input was echoed unmodified in the application's response. This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. Issue background Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request which, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application. The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes. Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site which causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method). The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality which it contains, and the other applications which belong to the same domain and organisation. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain which can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organisation which owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application, and exploiting users' trust in the organisation in order to capture credentials for other applications which it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk. Issue remediation In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defences: Input should be validated as strictly as possible on arrival, given the kind of content which it is expected to contain.

For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitised. User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > ' and =, should be replaced with the corresponding HTML entities (< > etc). In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

### Exploit Example:

```
Request
GET /wp-admin/admin.php?page=better_wp_security HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0)
Gecko/20100101 Firefox/11.0a7123<script>alert(1)</script>78089b4648b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Proxy-Connection: keep-alive
Referer: http://127.0.0.1/wp-admin/options-general.php
Cookie:
wordpress_5c016e8f0f95f039102cbe8366c5c7f3=admin%7C1333587813%7C73fe3e4d525d2460588947c4b7a03114;
wp-settings-1=widgets_access%3Doff%26uploader%3D1;
wp-settings-time-1=1333368822; wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_5c016e8f0f95f039102cbe8366c5c7f3=admin%7C1333587813%7C7b961d6e5caea2c784f282c5ed426964;
bb2_screener_=1333415711+127.0.0.1; PHPSESSID=j3l493obmaug7akebg8g3jb4k3
```

```
Response
HTTP/1.1 200 OK
Date: Tue, 03 Apr 2012 02:05:00 GMT
Server: Apache/2.2.20 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.6
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Last-Modified: Tue, 03 Apr 2012 02:05:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 35849
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<!--[if IE 8]>
<html xmlns="http://www.w3.org/1999/xhtml" class="ie8" dir="ltr" lang="en-US">
<![endif]-->
<!--[if !(IE 8) ]><!--
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr"
...[SNIP]...
<strong>Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0)
Gecko/20100101
Firefox/11.0a7123<script>alert(1)</script>[Injected Script]78089b4648b</strong>
```

#### Solution

Better Sanitization to eliminate possible XSS attacks

#### Issue Tracking URL

---

#### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fbetter-wp-security&old=542852&new\\_path=%2Fbetter-wp-security&new=542852](http://plugins.trac.wordpress.org/changeset?old_path=%2Fbetter-wp-security&old=542852&new_path=%2Fbetter-wp-security&new=542852)

## CVE-2012-3576

#### Context

Unrestricted file upload vulnerability in php/upload.php in the wpStoreCart plugin before 2.5.30 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in uploads/wpstystorecart.

#### Problem

wpStoreCart plugin for WordPress could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions by the upload.php script. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious PHP script, which could allow the attacker to execute arbitrary PHP code on the vulnerable system.

#### Solution

validate file extensions

#### Issue Tracking URL

---

#### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fwpstorecart&old=555124&new\\_path=%2Fwpstorecart&new=555124](http://plugins.trac.wordpress.org/changeset?old_path=%2Fwpstorecart&old=555124&new_path=%2Fwpstorecart&new=555124)

## CVE-2012-2920

#### Context

Cross-site scripting (XSS) vulnerability in the userphoto\_options\_page function in user-photo.php in the User Photo plugin before 0.9.5.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PATH\_INFO to wp-admin/options-general.php. NOTE: some of these details are obtained from third party information.

#### Problem

User Photo plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the options-general.php script. A remote attacker could exploit this vulnerability using the '\$\_SERVER['REQUEST\_URI']' parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

#### Solution

escape url before use

#### Issue Tracking URL

---

#### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fuser-photo&old=541880&new\\_path=%2Fuser-photo&new=541880](http://plugins.trac.wordpress.org/changeset?old_path=%2Fuser-photo&old=541880&new_path=%2Fuser-photo&new=541880)

## CVE-2012-2916

### Context

Cross-site scripting (XSS) vulnerability in sabre\_class\_admin.php in the SABRE plugin before 2.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the active\_option parameter to wp-admin/tools.php.

### Problem

SABRE plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the tools.php script. A remote attacker could exploit this vulnerability using the active\_option parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

### Solution

sanitize text before using it.

### Issue Tracking URL

---

### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fsabre&old=534490&new\\_path=%2Fsabre&new=534490](http://plugins.trac.wordpress.org/changeset?old_path=%2Fsabre&old=534490&new_path=%2Fsabre&new=534490)

## CVE-2012-2759

### Context

Cross-site scripting (XSS) vulnerability in login-with-ajax.php in the Login With Ajax (aka login-with-ajax) plugin before 3.0.4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the callback parameter in a lostpassword action to wp-login.php.

### Problem

Login With Ajax plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the login-with-ajax.php script. A remote attacker could exploit this vulnerability using the JSON callback parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

### Solution

Sanitize data before use

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset/541069>

## CVE-2012-2402

### Context

wp-admin/plugins.php in WordPress before 3.3.2 allows remote authenticated site administrators to bypass intended access restrictions and deactivate network-wide plugins via unspecified vectors.

### Problem

WordPress could allow a remote attacker to bypass security restrictions, caused by an error in plugins.php when handling network wide plugins. A remote attacker could exploit this vulnerability to bypass security restrictions and gain unauthorized administrative access to the vulnerable application.

### Solution

check that the authenticated user is a wp admin before allowing them to disable plugins

### Issue Tracking URL

---

### Commit URL

- <http://core.trac.wordpress.org/changeset/20526/branches/3.3/wp-admin/plugins.php>

## CVE-2012-1785

### Context

kg\_callffmpeg.php in the Video Embed & Thumbnail Generator plugin before 2.0 for WordPress allows remote attackers to execute arbitrary commands via unspecified vectors.

### Problem

Video Embed & Thumbnail Generator plugin for WordPress could allow a remote attacker to execute arbitrary code on the system, caused by the improper validation of user-supplied input in exec() function by the kg\_callffmpeg.php script. By persuading a victim to visit a specially-crafted Web page, a remote attacker could exploit this vulnerability to inject and execute arbitrary shell code on the vulnerable system.

### Solution

validate input before using

### Issue Tracking URL

---

### Commit URL

- [http://plugins.trac.wordpress.org/changeset?old\\_path=%2Fvideo-embed-thumbnail-generator&old=507924&new\\_path=%2Fvideo-embed-thumbnail-generator&new=507924](http://plugins.trac.wordpress.org/changeset?old_path=%2Fvideo-embed-thumbnail-generator&old=507924&new_path=%2Fvideo-embed-thumbnail-generator&new=507924)

## CVE-2012-1205

### Context

PHP remote file inclusion vulnerability in relocate-upload.php in Relocate Upload plugin before 0.20 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.

### Problem

Allowed anybody in include remote files

### Solution

Adopted proper 'wp\_ajax\_...' action, to close off a major security issue. only admin should have access to certain actions ('wp\_ajax\_relocate\_upload', 'relocate\_upload\_js\_action')

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset/504380/relocate-upload>

## CVE-2012-1125

### Context

Unrestricted file upload vulnerability in uploadify/scripts/uploadify.php in the Kish Guest Posting plugin before 1.2 for WordPress allows remote attackers to execute arbitrary code by uploading a file with a PHP extension, then accessing it via a direct request to the file in the directory specified by the folder parameter.

### Problem

Kish Guest Posting plugin for WordPress could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions by the uploadify.php script. By sending a direct request using the folder parameter, a remote attacker could exploit this vulnerability to upload a malicious PHP script, which could allow the attacker to execute arbitrary PHP code on the vulnerable system.

### Solution

Check the extension of the file to make sure its an allowable type. Do not allow folder creation.

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset/403694/kish-guest-posting/trunk/uploadify/scripts/uploadify.php>

## CVE-2012-1068

### Context

Cross-site scripting (XSS) vulnerability in the rc\_ajax function in core.php in the WP-RecentComments plugin before 2.0.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter, related to AJAX paging.

### Problem

WP-RecentComments Plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the core.php script. A remote attacker could exploit this vulnerability using the page parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

### Solution

sanitize input (make sure page is an int) before using the data.

### Issue Tracking URL

---

### Commit URL

- [http://plugins.trac.wordpress.org/changeset/416723/wp-recentcomments/trunk/core.php?old=316325&old\\_path=wp-recentcomments%2Ftrunk%2Fcore.php](http://plugins.trac.wordpress.org/changeset/416723/wp-recentcomments/trunk/core.php?old=316325&old_path=wp-recentcomments%2Ftrunk%2Fcore.php)

## CVE-2012-1011

### Context

actions.php in the AllWebMenus plugin 1.1.8 for WordPress allows remote attackers to bypass intended access restrictions to upload and execute arbitrary PHP code by setting the HTTP\_REFERER to a certain value, then uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.

### Problem

WordPress AllWebMenus Plugin could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions by the actions.php script. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious PHP script, which could allow the attacker to execute arbitrary PHP code on the vulnerable system. lack of checks in script actions.php allowed malicious user to upload any file to the vulnerable server. Create a file (For example, Wordpress\_security.php, with this content: echo <php echo '6Scan to the rescue'; ?>. Compress it with zip to awm.zip

### Solution

checks the source referrer

### Issue Tracking URL

---

### Commit URL

---

## CVE-2012-1010

### Context

Unrestricted file upload vulnerability in actions.php in the AllWebMenus plugin before 1.1.8 for WordPress allows remote attackers to execute arbitrary PHP code by uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.

**Problem**

WordPress AllWebMenus Plugin could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions by the actions.php script. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious PHP script, which could allow the attacker to execute arbitrary PHP code on the vulnerable system. lack of checks in script actions.php allowed malicious user to upload any file to the vulnerable server.

**Solution**

checks the source referrer,

**Issue Tracking URL**

---

**Commit URL**

---

## CVE-2012-0934

**Context**

PHP remote file inclusion vulnerability in ajax/savetag.php in the Theme Tuner plugin for WordPress before 0.8 allows remote attackers to execute arbitrary PHP code via a URL in the tt-abspath parameter.

**Problem**

WordPress Theme Tuner Plugin could allow a remote attacker to include arbitrary files. A remote attacker could send a specially-crafted URL request to the savetag.php script using the tt-abspath parameter to specify a malicious file from a remote system, which could allow the attacker to execute arbitrary code on the vulnerable Web server.

**Solution**

sanitize data before using it

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/492167/theme-tuner#file2>

## CVE-2011-5264

**Context**

Cross-site scripting (XSS) vulnerability in lazyest-backup.php in the Lazyest Backup plugin before 0.2.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the xml\_or\_all parameter

**Problem**

Lazyest Backup Plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using the xml\_or\_all parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

**Solution**

sanitize input before using it

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=470737%40lazyest-backup&old=468541%40lazyest-backup>

## CVE-2011-5226

**Context**

Cross-site request forgery (CSRF) vulnerability in wordpress\_sentinel.php in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to hijack the authentication of an administrator for requests that trigger snapshots.

**Problem**

Sentinel Plugin for WordPress is vulnerable to cross-site request forgery, caused by improper validation of user-supplied input. By persuading an authenticated user to visit a malicious Web site, a remote attacker could send a malformed HTTP request to perform unauthorized actions. An attacker could exploit this vulnerability to perform cross-site scripting attacks, Web cache poisoning, and other malicious activities.

**Solution**

escape html before using the input (sanitize)

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=475315@wordpress-sentinel&old=474998@wordpress-sentinel>

## CVE-2011-5225

**Context**

Cross-site scripting (XSS) vulnerability in wordpress\_sentinel.php in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via unknown vectors.

**Problem**

Sentinel Plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could

use this vulnerability to steal the victim's cookie-based authentication credentials.

**Solution**

sanitize input before use

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=475315@wordpress-sentinel&old=474998@wordpress-sentinel>

## CVE-2011-5224

**Context**

SQL injection vulnerability in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors.

**Problem**

Sentinel Plugin for WordPress is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements which could allow the attacker to view, add, modify or delete information in the back-end database.

**Solution**

validate data before using it for sql operations

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=475315@wordpress-sentinel&old=474998@wordpress-sentinel>

## CVE-2011-5216

**Context**

SQL injection vulnerability in ajax.php in SCORM Cloud For WordPress plugin before 1.0.7 for WordPress allows remote attackers to execute arbitrary SQL commands via the active parameter

**Problem**

SCORM Cloud for WordPress is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements to the ajax.php script using the active parameter, which could allow the attacker to view, add, modify or delete information in the back-end database.

**Solution**

validate data before performing sql operations

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/435356/scormcloud>

## CVE-2011-5194

**Context**

Cross-site scripting (XSS) vulnerability in vendors/samswhois/samswhois.inc.php in the Whois Search plugin before 1.4.2.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via the domain parameter, a different vulnerability than CVE-2011-5193.

**Problem**

The domain parameter allows for XSS

**Solution**

Validate input around the domain parameter

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/482954/wordpress-whois-search>

## CVE-2011-5192

**Context**

Cross-site scripting (XSS) vulnerability in pretty-bar.php in Pretty Link Lite plugin before 1.5.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the slug parameter, a different vulnerability than CVE-2011-5191.

**Problem**

Characters are not escaped around the slug parameter and allows for XSS.

**Solution**

Fixed a cross-site scripting vulnerability that could have affected a very small number of users Fix XSS near the slug parameter

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset/485819/pretty-link>

## CVE-2011-5191

### Context

Cross-site scripting (XSS) vulnerability in pretty-bar.php in Pretty Link Lite plugin before 1.5.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the slug parameter, a different vulnerability than CVE-2011-5192.

### Problem

Pretty link lite plugin allows XSS through via the slug parameter

### Solution

Fixed an issue with Pretty Link Export link for Pro users check input to make sure XSS is not possible

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset/473693/pretty-link>

## CVE-2011-5181

### Context

Cross-site scripting (XSS) vulnerability in clickdesk.php in ClickDesk Live Support - Live Chat plugin 2.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cdwidgetid parameter. NOTE: some of these details are obtained from third party information.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/36338/> ClickDesk Live Support plugin for WordPress is prone to a cross-site-scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. [http://www.example.com/\[path\]/wp-content/plugins/clickdesk-live-support-chat/clickdesk.php?cdwidgetid=\[xss\]](http://www.example.com/[path]/wp-content/plugins/clickdesk-live-support-chat/clickdesk.php?cdwidgetid=[xss])

### Solution

Not found

### Issue Tracking URL

---

### Commit URL

---

## CVE-2011-5180

### Context

Cross-site scripting (XSS) vulnerability in wp-1pluginjquery.php in the ZooEffect plugin 1.01 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter. NOTE: some of these details are obtained from third party information. NOTE: this has been disputed by a third party.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/36323/> 1-jquery-photo-gallery-slideshow-flash plug-in for WordPress is prone to a cross-site-scripting vulnerability because it fails to sufficiently sanitize user-supplied data. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. [http://www.example.com/\[path\]/wp-content/plugins/1-jquery-photo-gallery-slideshow-flash/wp-1pluginjquery.php?page=\[xss\]](http://www.example.com/[path]/wp-content/plugins/1-jquery-photo-gallery-slideshow-flash/wp-1pluginjquery.php?page=[xss])

### Solution

Not found

### Issue Tracking URL

---

### Commit URL

---

## CVE-2011-5128

### Context

Multiple cross-site scripting (XSS) vulnerabilities in the Adminimize plugin before 1.7.22 for WordPress allow remote attackers to inject arbitrary web script or HTML via the page parameter to (1) inc-options/deinstall\_options.php, (2) inc-options/theme\_options.php, or (3) inc-options/im\_export\_options.php, or the (4) post or (5) post\_ID parameters to adminimize.php, different vectors than CVE-2011-4926.

### Problem

Adminimize plugin does not escape html attributes in several parameters which enables users to perform XSS

### Solution

Escape html attributes in user input

### Issue Tracking URL

---

### Commit URL

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=467338@adminimize&old=466900@adminimize#file5>

## CVE-2011-5107

**Context**

Cross-site scripting (XSS) vulnerability in post\_alert.php in Alert Before Your Post plugin, possibly 0.1.1 and earlier, for WordPress allows remote attackers to inject arbitrary web script or HTML via the name parameter.

**Problem**

(Based on exploit)

"Alert Before Your Post" plugin for WordPress is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. [http://www.example.com/\[path\]/wp-content/plugins/alert-before-your-post/trunk/post\\_alert.php?name=\[xss\]](http://www.example.com/[path]/wp-content/plugins/alert-before-your-post/trunk/post_alert.php?name=[xss])

**Solution**

Properly Sanitize Input

**Issue Tracking URL**

---

**Commit URL**

---

## CVE-2011-5106

**Context**

Cross-site scripting (XSS) vulnerability in edit-post.php in the Flexible Custom Post Type plugin before 0.1.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the id parameter.

**Problem**

When querying the id of the post, the Flexible Custom Type Plugin doesn't make sure the id is an integer, which allows users to perform XSS

**Solution**

Make sure the id of the post is an integer

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=466252%40flexible-custom-post-type&old=465583%40flexible-custom-post-type>

## CVE-2011-5104

**Context**

Cross-site scripting (XSS) vulnerability in wpsc-admin/display-sales-logs.php in WP e-Commerce plugin 3.8.7.1 and possibly earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the custom\_text parameter.

**Problem**

The custom-text parameter input is not escaped for html attributes which causes the potential for XSS

**Solution**

Escape the html attributes in custom-text parameter

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=463447%40wp-e-commerce&old=463446%40wp-e-commerce>

## CVE-2011-4926

**Context**

Cross-site scripting (XSS) vulnerability in adminimize/adminimize\_page.php in the Adminimize plugin before 1.7.22 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.

**Problem**

The user input in page parameter is not escaped which causes the potential for XSS

**Solution**

Escape user input in page parameter

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=467338@adminimize&old=466900@adminimize#file5>

## CVE-2011-4803

**Context**

SQL injection vulnerability in wptouch/ajax.php in the WPtouch plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.

**Problem**

The id variable is not checked if it's an id number, which causes the potential to execute arbitrary SQL commands.

**Solution**

sanitize user input

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2011-4673****Context**

SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.

**Problem**

Based on exploit The id parameter is not checked if it's a valid id number, which causes the potential to execute arbitrary SQL commands

**Solution**

Sanitize User input

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2011-4671****Context**

SQL injection vulnerability in adrotate/adrotate-out.php in the AdRotate plugin 3.6.6, and other versions before 3.6.8, for WordPress allows remote attackers to execute arbitrary SQL commands via the track parameter (aka redirect URL).

**Problem**

Based on exploit \$wpdb->prepare can be misused to include a query, since no check is implemented on it.

**Solution**

Not found

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2011-4646****Context**

SQL injection vulnerability in wp-postratings.php in the WP-Post Ratings plugin 1.50, 1.61, and probably other versions before 1.62 for WordPress allows remote authenticated users with the Author role to execute arbitrary SQL commands via the id attribute of the ratings shortcode when creating a post. NOTE: some of these details are obtained from third party information.

**Problem**

In the rating attribute, the input provided by the user was not escaped which caused the potential for code injection

**Solution**

Escape the html attributes in the rating attribute

**Issue Tracking URL**

---

**Commit URL**

- [http://plugins.trac.wordpress.org/changeset/430970/wp-postratings/trunk/wp-postratings.php?old=355076&old\\_path=wp-postratings%2Ftrunk%2Fwp-postratings.php](http://plugins.trac.wordpress.org/changeset/430970/wp-postratings/trunk/wp-postratings.php?old=355076&old_path=wp-postratings%2Ftrunk%2Fwp-postratings.php)

**CVE-2011-4618****Context**

Cross-site scripting (XSS) vulnerability in advancedtext.php in Advanced Text Widget plugin before 2.0.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.

**Problem**

Characters received by the user for page parameter are not being escaped which causes the potential for XSS

**Solution**

Escape characters from user input

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=466102@advanced-text-widget&old=465828@advanced-text-widget>

**CVE-2011-4568**

**Context**

Cross-site scripting (XSS) vulnerability in view/frontend-head.php in the Flowplayer plugin before 1.2.12 for WordPress allows remote attackers to inject arbitrary web script or HTML via the URI.

**Problem**

[VAGUE] the Requested URI from the Server was not being encoded, which created the option for users to XSS through this parameter.

**Solution**

Encode the requested URI

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=413607%40fv-wordpress-flowplayer&old=409594%40fv-wordpress-flowplayer>

**CVE-2011-4562****Context**

Multiple cross-site scripting (XSS) vulnerabilities in (1) view/admin/log\_item.php and (2) view/admin/log\_item\_details.php in the Redirection plugin 2.2.9 for WordPress allow remote attackers to inject arbitrary web script or HTML via the Referer HTTP header in a request to a post that does not exist.

**Problem**

In multiple files, characters provided by the user are not escaped which causes the potential for XSS

**Solution**

Escape characters from user input to disable XSS

**Issue Tracking URL**

---

**Commit URL**

- <http://plugins.trac.wordpress.org/changeset?reponame=&new=447262%40redirection&old=421721%40redirection>

**CVE-2011-4342****Context**

PHP remote file inclusion vulnerability in wp\_xml\_export.php in the BackWPup plugin before 1.7.2 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the wpabs parameter.

**Problem**

A vulnerability has been discovered in the Wordpress plugin BackWPup 1.6.1 which can be exploited to execute local or remote code on the web server. The Input passed to the component "wp\_xml\_export.php" via the "wpabs" variable allows the inclusion and execution of local or remote PHP files as long as a "\_nonce" value is known. The "\_nonce" value relies on a static constant which is not defined in the script meaning that it defaults to the value "822728c8d9".

**Solution**

Not found

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2011-3981****Context**

PHP remote file inclusion vulnerability in actions.php in the Allwebmenus plugin 1.1.3 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.

**Problem**

Attackers can execute PHP in header paths since there is no check if the file being attached exists locally and there is no escaping of characters.

**Solution**

Add a check to see if the file exists locally and escape certain characters.

**Issue Tracking URL**

---

**Commit URL**

- [http://plugins.trac.wordpress.org/changeset/438959/allwebmenus-wordpress-menu-plugin/trunk/actions.php?old=408304&old\\_path=allwebmenus-wordpress-menu-plugin%2Ftrunk%2Factions.php](http://plugins.trac.wordpress.org/changeset/438959/allwebmenus-wordpress-menu-plugin/trunk/actions.php?old=408304&old_path=allwebmenus-wordpress-menu-plugin%2Ftrunk%2Factions.php)

**CVE-2011-1047****Context**

Multiple SQL injection vulnerabilities in VastHTML Forum Server (aka ForumPress) plugin 1.6.1 and 1.6.5 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) search\_max parameter in a search action to index.php, which is not properly handled by wpf.class.php, (2) id parameter in an editpost action to index.php, which is not properly handled by wpf-post.php, or (3) topic parameter to feed.php.

**Problem**

Based on exploit: <https://www.exploit-db.com/exploits/16235/> The vulnerability exists due to failure in the "index.php" script to properly sanitize user-supplied input in "search\_max" variable. Attacker can alter queries to the application SQL database, execute arbitrary queries to the database, compromise the application, access or modify sensitive data, or exploit various vulnerabilities in the underlying SQL database.

**Solution**

Sanitize user input

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2010-5295****Context**

Cross-site scripting (XSS) vulnerability in wp-admin/plugins.php in WordPress before 3.0.2 might allow remote attackers to inject arbitrary web script or HTML via a plugin's author field, which is not properly handled during a Delete Plugin action.

**Problem**

The name and author field of a plugin could inject code which would be executed when trying to delete a plugin.

**Solution**

Escape correctly the strings of name and author fields when trying to delete a plugin, so that they're safe to be used in HTML.

**Issue Tracking URL**

---

**Commit URL**

- <https://core.trac.wordpress.org/changeset/16373>

**CVE-2010-4839****Context**

SQL injection vulnerability in the Event Registration plugin 5.32 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the event\_id parameter in a register action.

**Problem**

Based on exploit The event\_id parameter is not checked properly, which enables users to inject SQL commands through it.

**Solution**

Based on exploit: sanitize user input

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2010-4747****Context**

Cross-site scripting (XSS) vulnerability in wordpress-processing-embed/data/popup.php in the Processing Embed plugin 0.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the pluginurl parameter.

**Problem**

Based on exploit: <https://www.exploit-db.com/exploits/35066/> The Processing Embed plugin for Wordpress is prone to a cross-site-scripting vulnerability because it fails to properly sanitize user-supplied input in pluginurl parameter. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.

**Solution**

Based on exploit: sanitize user input

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2010-4518****Context**

Cross-site scripting (XSS) vulnerability in wp-safe-search/wp-safe-search-jx.php in the Safe Search plugin 0.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the v1 parameter.

**Problem**

Based on exploit: <https://www.exploit-db.com/exploits/35067/> The Safe Search plugin for Wordpress is prone to a cross-site-scripting vulnerability because it fails to properly sanitize user-supplied input in v1 parameter. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.

**Solution**

Based on exploit: sanitize user input

**Issue Tracking URL**

---

**Commit URL**

---

## CVE-2010-3977

### Context

Multiple cross-site scripting (XSS) vulnerabilities in wp-content/plugins/cforms/lib\_ajax.php in cforms WordPress plugin 11.5 allow remote attackers to inject arbitrary web script or HTML via the (1) rs and (2) rsargs[] parameters.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/34946/> The cformsII plugin for WordPress is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input. An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and launch other attacks.

### Solution

Based on exploit: sanitize user data

### Issue Tracking URL

---

### Commit URL

---

## CVE-2010-2924

### Context

SQL injection vulnerability in myLDlinker.php in the myLinksDump Plugin 1.2 for WordPress allows remote attackers to execute arbitrary SQL commands via the url parameter.

### Problem

Based on exploit The URL parameter is not validated properly, which enables users to inject SQL commands through it.

### Solution

Not found

### Issue Tracking URL

---

### Commit URL

---

## CVE-2010-1186

### Context

Cross-site scripting (XSS) vulnerability in xml/media-rss.php in the NextGEN Gallery plugin before 1.5.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the mode parameter.

### Problem

Based on exploit. This vulnerability results from reflected unsanitized input that can be crafted into an attack by a malicious user by manipulating the mode parameter of the xml/media-rss.php script. This vulnerability is triggered because the mode parameter on the media-rss.php script is not correctly escaped to avoid HTML code injection. \$mode = \$\_GET["mode"]; This parameter is reflected back to the user if no correct mode is selected. } else { header('content-type:text/plain;charset=utf-8'); echo sprintf(\_\_("Invalid MediaRSS command (%s).", "nggallery"), \$mode); exit; } It's worth to note that the Content-Type is chosen safely by the plugin, but this is not enough to avoid code injection because some browsers (most notably Microsoft Internet Explorer) choose the content type by parsing the content the web-server returns instead of obeying the proper headers.

### Solution

Base on exploit: sanitize data

### Issue Tracking URL

---

### Commit URL

---

## CVE-2010-0673

### Context

SQL injection vulnerability in cplphoto.php in the Copperleaf Photolog plugin 0.16, and possibly earlier, for WordPress allows remote attackers to execute arbitrary SQL commands via the postid parameter.

### Problem

The postid parameter is not validated properly, which causes the potential to inject SQL commands through it.

### Solution

Not found

### Issue Tracking URL

---

### Commit URL

---

## CVE-2009-4748

**Context**

SQL injection vulnerability in mycategoryorder.php in the My Category Order plugin 2.8 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the parentId parameter in an act\_OrderCategories action to wp-admin/post-new.php.

**Problem**

Based on exploit My Category Order plugin does not check if the id for a query parameter is integer, which enables attackers to inject SQL commands

**Solution**

Based on exploit Check if the id is integer

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2009-4672****Context**

Directory traversal vulnerability in main.php in the WP-Lytebox plugin 1.3 for WordPress allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the pg parameter.

**Problem**

Based on exploit Directory traversal can be performed through the pg parameter through '..' which may give users access to files.

**Solution**

Not found.

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2009-4424****Context**

SQL injection vulnerability in results.php in the Pyrmont plugin 2 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.

**Problem**

Based on exploit The id parameter is not validated properly, which causes the potential for users to inject SQL commands through it.

**Solution**

Base on exploit: sanitize user input

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2009-2396****Context**

PHP remote file inclusion vulnerability in template/album.php in DM Albums 1.9.2, as used standalone or as a WordPress plugin, allows remote attackers to execute arbitrary PHP code via a URL in the SECURITY\_FILE parameter.

**Problem**

Based on exploit:  
Security File parameter is not validated properly and can include php files, which causes the potential for arbitrary code execution

**Solution**

Not found

**Issue Tracking URL**

---

**Commit URL**

---

**CVE-2009-2383****Context**

SQL injection vulnerability in BTE\_RW\_webajax.php in the Related Sites plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the guid parameter.

**Problem**

Based on exploit Guid parameter is not validated properly which enables users to perform SQL Injection

**Solution**

Not provided

**Issue Tracking URL**

---

**Commit URL**

---

## CVE-2009-2334

### Context

wp-admin/admin.php in WordPress and WordPress MU before 2.8.1 does not require administrative authentication to access the configuration of a plugin, which allows remote attackers to specify a configuration file in the page parameter to obtain sensitive information or modify this file, as demonstrated by the (1) collapsing-archives/options.txt, (2) akismet/readme.txt, (3) related-ways-to-take-action/options.php, (4) wp-security-scan/securityscan.php, and (5) wp-ids/ids-admin.php files.

NOTE: this can be leveraged for cross-site scripting (XSS) and denial of service.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/9110/>

A vulnerability was found in the way that WordPress handles some URL requests. This results in unprivileged users viewing the content of plugins configuration pages, and also in some plugins modifying plugin options and injecting JavaScript code. Arbitrary native code may be run by a malicious attacker if the blog administrator runs injected JavaScript code that edits blog PHP code. No privileges are checked on WordPress plugins configuration PHP modules using parameter 'page' when we replace 'options-general.php' with 'admin.php'. The same thing happens when replacing other modules such as 'plugins.php' with 'admin.php'. Basic information disclosure is done this way. For example, with the following URL a user with no privileges can see the configuration of plugin Collapsing Archives, if installed.  
[http://\[some\\_wordpress\\_blog\]/wp-admin/admin.php?page=/collapsing-archives/options.txt](http://[some_wordpress_blog]/wp-admin/admin.php?page=/collapsing-archives/options.txt)

### Solution

Not found.

### Issue Tracking URL

---

### Commit URL

---

## CVE-2009-2122

### Context

SQL injection vulnerability in viewimg.php in the Paolo Palmonari Photoracer plugin 1.0 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/8961/> Id parameter in plugin not validated, which enables users to inject SQL

### Solution

Not provided

### Issue Tracking URL

---

### Commit URL

---

## CVE-2009-0968

### Context

SQL injection vulnerability in fmoblog.php in the fMoblog plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php. NOTE: some of these details are obtained from third party information.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/8229/> Page id parameter is not validated properly, which enables users to inject SQL using it

### Solution

Not provided

Based on exploit: sanitize data

### Issue Tracking URL

---

### Commit URL

---

## CVE-2008-6811

### Context

Unrestricted file upload vulnerability in image\_processing.php in the e-Commerce Plugin 3.4 and earlier for Wordpress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in wp-content/plugins/wp-shopping-cart/.

### Problem

An e-Commerce plugin allows to upload executable files and to modify the we-shopping-cart directory which causes the potential for executing arbitrary code.

It is possible to upload a selected file to the ... /wp-content/plugins/wp-shopping-cart/ directory. If the directory is not writable (rare cases) you can use the insecure GET variable "imagedir" to directory traversal so you can upload in different directories.

### Solution

Not provided.

### Issue Tracking URL

---

### Commit URL

---

## CVE-2008-5752

### Context

Directory traversal vulnerability in getConfig.php in the Page Flip Image Gallery plugin 0.2.2 and earlier for WordPress, when magic\_quotes\_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the book\_id parameter. NOTE: some of these details are obtained from third party information.

### Problem

Based on exploit book\_id parameter can be used to traverse directories through .. /wp-content/plugins/page-flip-image-gallery/books/getConfig.php?  
book\_id=../../../../../../../../etc/passwd%00123

### Solution

Not found

### Issue Tracking URL

---

### Commit URL

---

## CVE-2008-5695

### Context

wp-admin/options.php in WordPress MU before 1.3.2, and WordPress 2.3.2 and earlier, does not properly validate requests to update an option, which allows remote authenticated users with manage\_options and upload\_files capabilities to execute arbitrary code by uploading a PHP script and adding this script's pathname to active\_plugins.

### Problem

WordPress is prone to a vulnerability that lets remote attackers execute arbitrary code because the application fails to sanitize user-supplied input. Attackers can exploit this issue to execute arbitrary PHP code within the context of the affected webserver process.

### Solution

WordPress allows any user with manage\_options capability to update directly any blog's option through wp-admin/options.php, so this feature can be used to perform (or hide) multiple attacks where WordPress expects safe data coming from the DB. This bug is very critical in those sites using WordPress MU, because any user has the manage\_options capability.

### Issue Tracking URL

---

### Commit URL

---

## CVE-2008-4625

### Context

SQL injection vulnerability in stnl\_iframe.php in the ShiftThis Newsletter (st\_newsletter) plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the newsletter parameter, a different vector than CVE-2008-0683.

### Problem

Based on exploit The newsletter parameter is not validated properly, which causes the potential to execute arbitrary SQL commands. [http://flymusic.co.uk/wp-content/plugins/st\\_newsletter/stnl\\_iframe.php?newsletter=-9999+UNION+SELECT+concat\(user\\_login,0x3a,user\\_pass,0x3a,user\\_email\)+FROM+wp\\_users--](http://flymusic.co.uk/wp-content/plugins/st_newsletter/stnl_iframe.php?newsletter=-9999+UNION+SELECT+concat(user_login,0x3a,user_pass,0x3a,user_email)+FROM+wp_users--)

### Solution

Not found

Based on Exploit: sanitize input

### Issue Tracking URL

---

### Commit URL

---

## CVE-2008-1982

### Context

SQL injection vulnerability in ss\_load.php in the Spreadsheet (wpSS) 0.6 and earlier plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the ss\_id parameter.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/5486/> The ss\_id parameter is not checked if it's an integer and is included in query, which creates the option for SQL injection

### Solution

Not found

Base on exploit: sanitize input

### Issue Tracking URL

---

### Commit URL

---

## CVE-2008-0491

### Context

SQL injection vulnerability in fim\_rss.php in the fGallery 2.4.1 plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the album parameter.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/4993/> album parameter is not escaped or neutralized.

### Solution

Not found

Based on exploit: escape parameter

### Issue Tracking URL

---

### Commit URL

---

## CVE-2007-5800

### Context

Only WordPress installations on hosts which allow for register\_globals = on allow\_url\_fopen = on in their php.ini settings are affected.

Multiple PHP remote file inclusion vulnerabilities in the BackUpWordPress 0.4.2b and earlier plugin for WordPress allow remote attackers to execute arbitrary PHP code via a URL in the bkpwp\_plugin\_path parameter to (1) plugins/BackUp/Archive.php; and (2) Predicate.php, (3) Writer.php, (4) Reader.php, and other unspecified scripts under plugins/BackUp/Archive/.

### Problem

[BASED ON EXPLOIT] The URL parameter is not validated properly and enables users to execute arbitrary PHP code. This is an instance of CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

### Solution

Not found

Based on exploit: properly validate url parameter

### Issue Tracking URL

---

### Commit URL

---

## CVE-2006-5705

### Context

WP-DB-Backup allows the backup of the core WordPress database tables.

Multiple directory traversal vulnerabilities in plugins/wp-db-backup.php in WordPress before 2.0.5 allow remote authenticated users to read or overwrite arbitrary files via directory traversal sequences in the (1) backup and (2) fragment parameters in a GET request.

### Problem

A directory traversal can be performed in backup and fragment parameters in GET requests, which enables users to read or overwrite files through plugins. [CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')]

### Solution

Validate backup and fragment parameters to not allow directory traversal. In short, it verifies whether the GET parameters "backup" and "fragment" do not have traversal characters (such as .. or ./ etc)

### Issue Tracking URL

---

### Commit URL

- <http://trac.wordpress.org/changeset/4226>

# Chromium

---

## [CVE-2016-1650](#)

### Context

The flaw occurs in an [API used by extensions](#) for doing a page capture

### Problem

There is a [race condition](#), when a failure occurs in the PageCaptureSaveAsMHTMLFunction extension function (pageCapture.saveAsMHTML). There are a [few different ways the use-after-free](#) can occur, but suppose we have the following background extension script: chrome.pageCapture.saveAsMHTML({ "tabId": 1337 }, function(results) {}); When this function's RunAsync() is called, a single AddRef() is called to add an additional reference to the function. This is "balanced" with a Release() in ReturnFailure(), and in OnMessageReceived(). The problem is that [it's possible for both Release\(\)s to be called causing a race condition and a uaf crash.](#)

### Solution

[Remove extra Release\(\) in pageCapture extension function](#) implementation.

### Codes

"Application crash", "Race condition"

---

## [CVE-2016-1640](#)

### Context

The Web Store inline-installer implementation in the Extensions UI in Google Chrome before 49.0.2623.75 [does not block installations](#) upon deletion of an installation frame, which [makes it easier for remote attackers to trick a user](#) into believing that an installation [request originated from the user's next navigation](#) target via a crafted web site.

### Problem

An installation [can only trigger an extension install that is hosted in the same origin](#) of the site who triggered the install. This vulnerability [makes it possible to display an inline extension installation dialog on a different origin](#) that initiated the install. Thus [tricking the user into installing an Extension](#) as if it was from that origin. As the [dialog doesn't show the origin, it gives even more credibility to the attack.](#)

### Solution

[Don't allow inline install if frame is deleted before user accepts.](#) If the frame that called the chrome.webstore.install method to begin an inline install gets deleted before the user accepts from the dialog, we don't want the install to continue because a [navigation could make it look like the install request was coming from some unrelated site](#). One downside of this approach is that the dialog stays around even after the frame is deleted, and hitting either accept or cancel buttons both just cancel the install. It [would be better if the dialog is automatically cancelled, but doing that would involve a lot more refactoring](#). The approach in this CL was easier and is probably worth getting out, and we can improve on it in the future.

### Codes

"Installer", "Bypass protection mechanism", "Spoofed origin of an install request", "Tricking user into installing a malicious plug-in"

---

## [CVE-2016-1638](#)

## Context

**Restrictions can be bypassed**, which **allows remote attackers to bypass intended access restrictions** via a crafted platform app.

## Problem

Chrome Version: 48.0.2564.103 (stable, and earlier) and 50.0.2633.0 (HEAD) Some web platform APIs are disabled in Chrome apps for security reasons ([https://developer.chrome.com/apps/app\\_deprecated](https://developer.chrome.com/apps/app_deprecated)). This is implemented in platform\_app.js [1]. These **restrictions can be bypassed**: (I) The restriction of document.open/write/writeln/close is implemented by **shadowing HTMLDocument.prototype.write**, but Document.prototype.write should be shadowed instead.

So, either of the following two ways allows the use of the restricted API: delete HTMLDocument.prototype.write; Document.prototype.write.call(document); (II) window.onbeforeunload is shadowed by Object.defineProperty with configurable:true. This allows the property descriptor to be removed via the delete operator: delete window.onbeforeunload; // Remove restriction window.onbeforeunload = function() { return 'This should not be visible!'; }; PoC for I: See issue 585268 (document.write/close was used for that exploit). PoC for II: 1. Download manifest.json and background.js 2. Load the app (either via chrome://extensions, or by uploading it to the Chrome Web Store and installing it). 3. The app uses the above trick, and then calls location.reload() to show a PoC. Expected result: "window.onbeforeunload is not available in packaged apps." error in console. Actual result : Upon unload, a dialog shows up.

## Solution

It's easy enough to patch these particular issues - **disable the methods on Document instead of HTMLDocument**, don't do strict comparisons for onunload and related, remove the configurable, etc. The underlying problem though is that we're trying to mangle things in JS that really should **fundamentally be guaranteed at a lower level** (probably somewhere in blink). Unfortunately, I don't know the best way to begin going about that (or if it's even necessarily something we really want to do), and don't personally have time to implement it at the moment. If anyone knows a way that this is already done in blink (or content/, or v8), lemme know - in the meantime, I'll go ahead and make these fixes to at least harden our security a little bit.

## Codes

"Not enforcing private code", "Bypass protection mechanism"

---

## CVE-2016-1635

### Context

extensions::LoadWatcher::CallbackAndDie is called when DidCreateDocumentElement is triggered. CallbackAndDie calls a user-defined JavaScript function and then deletes the LoadWatcher instance. However, **JavaScript code can easily replace the document** (e.g. via document.close/write) and DidCreateDocumentElement is triggered also whenever a document is created/replaced.

### Problem

Malicious Chrome apps can cause CallbackAndDie to be called **re-entrantly**, when the callback of chrome.apps.window.create replaces the document of the new app window, which results in a use-after-free. This results in a **crash** of the Web browser.

### Solution

Avoid re-entrant calls by using **PostTask through observer notifications** that the method has been **called once and has not finished executing**.

### Codes

"Reentrancy", "Application crash", "Enforcing atomicity of event dispatching"

---

## CVE-2016-1622

### Context

The Object.defineProperty() method defines a new property directly on an object, or modifies an existing property on an object, and returns the object. It was being used as an attack vector.

### Problem

Malicious parties can change the content of an extension through its code being able to be accessed through Object.defineProperty method. This allows third parties to change the behavior of the extension through crafted Javascript code.

This results in a Same-Origin Policy bypass.

### Solution

Don't allow built-in extensions code to be overridden.

### Codes

"JS Objects Isolation", "Same-Origin Policy Bypass", "Alter Execution Logic"

---

## CVE-2015-6779

### Context

PDFium, as used in Google Chrome before 47.0.2526.73, does not properly restrict use of chrome: URLs, which allows remote attackers to bypass intended scheme restrictions via a crafted PDF document, as demonstrated by a document with a link to a chrome://settings URL.

### Problem

A hyperlink inside a pdf file shown by the chrome pdf-viewer can link to a chrome:// url and can be opened as a new tab. As this is prohibited in html (it will open about:blank), it also shouldn't be possible in a pdf-file. PDF viewer allows navigation to file:// URLs, whereas it does not for webpages.

### Solution

a mechanism for more granular link URL permissions (filtering on scheme/host). This fixes the bug that allowed PDFs to have working links to any "chrome://" URLs

### Codes

"Bypass protection mechanism", "Trigger access to an arbitrary URL"

---

## CVE-2015-6772

### Context

Security: Universal XSS using plugin objects Google chromium allows that elements are attached/detached at runtime using javascript. Each attached document in iframes is checked against the Same-Origin Policy.

### Problem

This is a regression from issue 524120. Now that widget updates are deferred until after the frame is detached from the document (and beyond the lifetime of ScriptForbiddenScope, too), it is possible to attach another document to the frame before a new document is installed. The attached document can then be used to bypass the same-origin policy. "So the root cause of this issue is that running nested message loops that invoke script in Document::detach() generally results in broken invariants. The original patch tries to change the timing of running deferred widget updates to the message loop, to

avoid re-entrancy. However, that [hit a lot of crashes](#) and didn't look like something that would be easy to merge to M47. Another patch:<https://codereview.chromium.org/1444183003> works but it turns out that it can leave a dangling Document/FrameView. The invariant being violated here is that [Frame has no FrameView at the end of Document::detach\(\)](#).

## Solution

"Note that the change looks large, but it's really just moving FrameNavigationDisabler from NavigationScheduler into LocalFrame. The [core change in the patch is just adding one line to Document::detach to disable navigations:](#) FrameNavigationDisabler navigationDisabler(\*m\_frame); Which is really [low risk](#) because prior to r350972, [these sorts of navigations couldn't be triggered anyway.](#)"

## Codes

"Reentrancy", "Same-Origin Policy Bypass", "Use after free"

---

## [CVE-2015-1302](#)

### Context

Security: Cross-site read access to PDF files. [Pdf Data leakage across cross-origin.](#)

### Problem

The [out-of-process viewer exposes an API](#) when its MIME-type is set to application/x-google-chrome-pdf, presumably to support the print preview.

Among the supported API is a [method to select all text and get the contents of the selection.](#) This [allows any web page to read the contents of a PDF file from any source.](#)

I have attached a proof of concept.

1. Open the page.
2. Input the URL of a PDF file (I've used the Bitcoin paper as an example).
3. Click on the "Show content" button.
4. The contents of the PDF will be displayed in the PDF.

This can be fully automated, websites could scan for popular URLs and automatically read the contents of a PDF. [The only defence for users is to disable plugin loading by default.](#) There are three settings, "Run all plugin content", "Detect and run important plugin content" and "Let me choose when to run plugin content". Only the last option protects users from this exploit.

## Solution

[insert an iframe](#) (containing a page from ChromeVox's origin) that [directly communicates with the PDF component extension](#), via a MessagePort. The [sender and receiver have to mutually authenticate each other](#), this [can be done by communicating a random value over another channel](#) (e.g. extension message passing API). - Run ChromeVox in the component extension, and [directly communicate between the component extension and ChromeVox.](#)

## Codes

"Same-Origin Policy Bypass", "Data leakage"

---

## [CVE-2015-1298](#)

### Context

The chrome.runtime is [exposed for app developers to access some information about the underlying runtime environment](#), as stated in the documentation: "Use the chrome.runtime API to retrieve the background page, return details

about the manifest, and listen for and respond to events in the app or extension lifecycle. You [can also use this API to convert the relative path of URLs to fully-qualified URLs](#)." Source: <https://developer.chrome.com/apps/runtime#method-setUninstallURL>

### Problem

chrome.runtime.setUninstallURL [only checks whether the given parameter is a syntactically valid URL](#), but it [does not enforce the blacklist of disallowed URLs](#). This [allows extensions and apps \(without requiring any install permissions\) to open any URL, including special chrome:// URLs](#). In the worst case, this bug [could be used to exploit a memory bug in the browser process](#) (e.g. UAF in a browser thread upon shutdown).

### Solution

To restrict chrome.runtime.setUninstallURL to http(s). [Disallow URLs other than http\(s\) in chrome.runtime.setUninstallURL](#). And [allow empty URLs to be set to clear the uninstallation URL](#). [Added an optional callback, to know when setting the URL finished \(or failed\)](#).

### Codes

"User-assisted attack", "Not enforcing permissions", "Trigger access to an arbitrary URL"

---

## CVE-2015-1297

### Context

The WebRequest API implementation in extensions/browser/api/web\_request/web\_request\_api.cc in Google Chrome before 45.0.2454.85 [does not properly consider a request's source before accepting the request](#), which allows remote attackers to [bypass intended access restrictions via a crafted \(1\) app or \(2\) extension](#).

### Problem

webRequest API allows extensions to [intercept and redirect requests from the browser](#). That [includes requests from other extensions](#). However, it also [allows to intercept XMLHttpRequest requests from Chrome Apps, which is quite possibly unintended](#). Chrome Apps are [supposed to be as much independent from the browser as possible](#).

### Solution

[Hide requests in an extension from other extensions](#)

### Codes

"Dispatching events to unauthorized listeners", "Extensions being able to tamper with other extensions"

---

## CVE-2015-1226

### Context

[Extensions API](#): The DebuggerFunction::InitAgentHost function in browser/extensions/api/debugger/debugger\_api.cc in Google Chrome before 41.0.2272.76 [does not properly restrict what URLs are available as debugger targets](#), which [allows remote attackers to bypass intended access restrictions via a crafted extension](#).

### Problem

[Extensions can silently debug](#) (run code) in [ANY tab and escape the sandbox](#). The chrome.debugger extension API [can attach to targets at any origin](#), including URLs such as file://, chrome://, chrome-extension:// and the Chrome Web store. [Attaching to privileged targets is usually forbidden when the target is specified by tabId or extensionId](#). However, it is also [possible to attach to a target by targetId, which is not subjected to any validation](#). This [targetId can easily](#) be obtained using the chrome.debugger.getTargets method. Because of these capabilities, [anything that can be displayed in a tab is completely compromised when a user installs an extension that exploits this bug](#).

## Solution

Validate debugger.targetId before use in chrome.debugger and refactored the tests to [make sure that the debugger is detached upon returning from RunAttachFunction](#). Previously, if the [debugger unexpectedly succeeded in attaching](#), the method would return (because empty error != some error), [causing the attached debugger to not be detached](#). In short, they [added a permission check](#)

## Codes

"Sandbox escape", "Bypass protection mechanism", "Not enforcing permissions", "Allowing extensions to debug tabs"

---

## CVE-2014-3172

### Context

The Debugger extension API in browser/extensions/api/debugger/debugger\_api.cc in Google Chrome before 37.0.2062.94 [does not validate a tab's URL before an attach operation](#), which [allows remote attackers to bypass intended access limitations](#) via an extension that [uses a restricted URL, as demonstrated by a chrome:// URL](#).

### Problem

[Any extension can debug any other extension](#), and be [able to maliciously use the data of users](#). By using the "downloads" permission in conjunction with network\_diag, network\_logging, wpa\_debug, and ff\_debug it [should be possible to snoop on a lot of private user data](#).

## Solution

Have the Debugger extension api [check that it has access](#) to the tab Check PermissionsData::CanAccessTab() [prior to attaching the debugger](#).

## Codes

"Bypass protection mechanism", "Lack of security checks", "Not enforcing permissions", "Extensions being able to tamper with other extensions"

---

## CVE-2014-3170

### Context

Extensions/common/url\_pattern.cc in Google Chrome before 37.0.2062.94 [does not prevent use of a '\0' character in a host name](#), which [allows remote attackers to spoof the extension permission dialog](#) by [relying on truncation after this character](#).

### Problem

By [inserting a NUL byte in a host permission](#), extension authors can [hide all host permission requests](#), giving users a [false sense of security when they install an extension](#).

## Solution

**Do not allow NUL characters in the hosts of host permissions.**

## Codes

"Privilege elevation", "Bypass protection mechanism", "Incorrect parsing of manifest file"

---

## CVE-2014-1728

### Context

**out of bounds writes** A Pwnium 4 entry **achieved a sandbox escape** by **sending messages from a compromised swapped out renderer to a vulnerable extension**. The problem seems to be in TabHelper, which is **getting state confused by the swap out**. creis' synopsis: **TabHelper is not deleting state associated with a swapped out RVH**. It should probably be listening to WebContentsObserver::RenderViewHostChanged in addition to RenderViewHostCreated.

### Problem

The exploit is **possible because the attacker's renderer process can send a message from a swapped out RenderFrameHost which makes it up into TabHelper**. TabHelper isn't keeping **track of who sent the message** and assumes it's from WebContents::GetRenderViewHost(), which refers to the current RenderViewHost (legitimately for the extension process) and not the swapped out one (in the attacker's process). Multiple things are wrong here: 1) A **message from a swapped out RFH is making it up to TabHelper**. **Swapped out hosts shouldn't be propagating their IPC messages up to observers**. We actually have a check for that in RenderViewHostImpl::OnMessageReceived, where we filter out such IPC messages using CanHandleWhileSwappedOut. We're **missing that check in RenderFrameHostImpl**, which is how this snuck through. Nasko will fix that. 2) **TabHelper doesn't know who sent it the message, since that information is not available in OnMessageReceived**. In theory, it would be nice for it not to have to worry about that, since it's easy to miss an access control check. Fixing (1) **means we don't have to worry about messages from swapped out RFHs**, for example. Unfortunately, the **problem still exists with current vs pending RFHs**. More concretely, a **WebContents can have both a current and a pending RFH at the same time** (e.g., one in an attacker's process and one in an extension process). Until the pending RFH actually commits, **IPC messages could come up to WebContentsObservers from either one**, and the **observers just assume that they're hearing from the current RFH, not the pending one. That could lead to the same kind of attack**.

### Solution

More concretely, a **WebContents can have both a current and a pending RFH at the same time** (e.g., one in an attacker's process and one in an extension process). Until the pending RFH actually commits, **IPC messages could come up to WebContentsObservers from either one, and the observers just assume that they're hearing from the current RFH, not the pending one**. That could lead to the same kind of attack. I'm not sure if it's possible to **hide messages from the pending RFH until it commits**, since it **may need to initialize state** (e.g., RenderFrameCreated) before the commit happens. **Queuing the messages up inside WebContents until commit** might be possible, but that feels really **error prone if it delays acks or other message exchanges**. Another option is to **expose who sent the IPC message so that the observer can do an access control check**. **Exposing "who sent it"** could be in the form of RenderFrameHost, routing ID + process ID, SiteInstance, or some kind of security principal. **Longer term efforts like Mojo might help** with that. In the shorter term, it's less clear how to fix that **without exposing concepts like pending RFHs to observers**.

## Codes

"Sandbox escape", "Added origin check", "IPC has no info about origin of a message"

---

## CVE-2013-2912

### Context

Heap-use-after-free in ppapi::proxy::PluginResource::NotifyInstanceWasDeleted. A **refactoring was suggested but reverted because it broke Docs print preview**. A little more printf debugging reveals that the **PluginResource destructor**

sends the destruct message to the host but never exits. It looks like a hang, but there shouldn't be multiple threads for in-process plugins.

## Problem

A unique situation for in-process plugins. The repro.html file causes a load to start, then a reload, then moves the plugin element when the ready state changes. The instance is torn down while we're in one of the URLLoaderResource dtors, before it has removed itself from the tracker. The resource tracker tries to use the object which is half destructed. The repro.html forces it into a state it doesn't like, hitting a NOTREACHED which needs to be changed.

## Solution

Change the PepperInProcessRouter to defer resource destruction messages. This changes the in process "proxy" so it posts tasks to send resource destruction messages instead of calling them directly. This prevents several kinds of re-entrancy into the plugin-side code. In this case, when a URLLoader is released, the plugin can finish before the host cancels the load and potentially deletes the instance.

## Codes

"Reentrancy", "Application crash"

---

## CVE-2013-2876

### Context

Extensions UI- browser/extensions/api/tabs/tabs\_api.cc in Google Chrome before 28.0.1500.71 does not properly enforce restrictions on the capture of screenshots by extensions, which allows remote attackers to obtain sensitive information about the content of a previous page via vectors involving an interstitial page.

## Problem

Extensions are allowed to screenshot interstitial websites content without having permission to do so, hence being able to steal user's information.

## Solution

Add check for permission screenshot even in interstitial websites or not allow it by default.

## Codes

"Data leakage", "Bypass protection mechanism", "Lack of security checks"

---

## CVE-2013-2868

### Context

common/extensions/sync\_helper.cc in Google Chrome before 28.0.1500.71 proceeds with sync operations for NPAPI extensions without checking for a certain plugin permission setting, which might allow remote attackers to trigger unwanted extension changes via unspecified vectors.

## Problem

Chrome Sync is used to install an extension with NPAPI plugin and execute code. Though extensions with plugins cannot be installed through sync directly, they can be auto-updated, and the new version may contain plugins. chrome/common/extensions/sync\_helper.cc checks PluginsInfo::HasPlugins to determine if an extension can be synced. HasPlugins returns false if there's an empty plugins section. chrome/common/extensions/api/plugins/plugins\_handler.cc parses "plugins" from the manifest. It reats an empty "plugins" section differently from it not being there, though. It also

[adds the "plugins" permission if there are any plugins](#); it should be [treated as a permissions increase](#) (disabling the extension) if there are new plugins in the new version of the extension.

## Solution

The fix [adds a check for IpluginI permission while syncing NPAPI plugins.](#)

## Codes

"Privilege elevation", "Bypass protection mechanism", "Plugin update"

---

## CVE-2013-2841

### Context

[Use-after-free vulnerability](#) allows remote attackers to cause a [denial of service](#) or possibly have unspecified other impact via vectors [related to the handling of Pepper resources](#). generic WebKit DOM vs. PPAPI URL loading lifetime issue.

### Problem

1. PPB\_URLLoader\_Impl(ppb\_url\_loader\_impl.h) is a subclass of ppapi::Resource(ppapi/shared\_impl/resource.h). 2. But for some strange reason [destructor of ppapi::Resource is not executed when destructor of PPB\\_URLLoader\\_Impl is executed](#). 3. Think that is why this bug happens. [Because destructor of ppapi::Resource should be executed to remove PPB\\_URLLoader\\_Impl instance from ResourceMap live resources of ResourceTracker\(ppapi/shared\\_impl/resource\\_tracker.cc\)](#). 4. [Otherwise PPB\\_URLLoader\\_Impl isntance will remain in ResourceMap live resources of ResourceTracker even after being deleted.](#)

## Solution

[Remove Pepper URLLoader from resource tracker early](#). This [protects against double delete](#) if the instance is destroyed as a result of canceling a load.

## Codes

"Application crash"

---

## CVE-2013-0925

### Context

Google Chrome before 26.0.1410.43 [does not ensure that an extension has the tabs \(aka APIPermission::kTab\) permission before providing a URL to this extension](#), which has unspecified impact and remote attack vectors.

### Problem

The chrome.tabs.onUpdated event is [accessible to Chrome extensions even without the "tabs" permission, and leaks the URLs the user navigates](#) to in the changeInfo.url argument to the event callback.

## Solution

[Do not pass URLs in onUpdated events to extensions unless they have the "tabs" permission.](#)

## Codes

"Steal data", "Dispatching events to unauthorized listeners"

---

## CVE-2013-0924

## Context

When you install an extension, there are warnings about host permissions. However, by design there aren't any for file: permissions - these are handled via a checkbox on the extension settings page. The same goes for the permissions API.

## Problem

The API implementation doesn't respect the checkbox value on the extensions settings page, so silently allows extensions to obtain file level permissions.

## Solution

The API implementation should check for the checkbox values by users in the extension settings page that regulate file: permissions.

## Codes

"Installer", "Incorrect warning of permissions", "Silently allows extensions to obtain file level permissions"

---

## CVE-2013-0910

### Context

Google Chrome before 25.0.1364.152 does not properly manage the interaction between the browser process and renderer processes during authorization of the loading of a plug-in, which makes it easier for remote attackers to bypass intended access restrictions via vectors involving a blocked plug-in.

### Problem

A compromised renderer can load banned plug. The renderer has the capability to block or unblock plug-in it, but having the decision of block/unblocking a plug-in in the renderer is weak: renderer interacts with content from the Web (untrusted) and may be compromised.

Therefore, a stronger decision is to have the checks of blocks/unblocked plug-ins in the browser-side.

- Allegedly, Java is installed on 66% of computers (largely independent of browser).
- A Java installation is frequently out of date; we block this situation.
- Even when up-to-date, Java is a security nightmare -- it's currently the largest source of severe 0-day attacks in the browser ecosystem. Because of this, we block even an up-to-date Java.

So, interestingly, now think about a compromised renderer. A compromised renderer gets to load any plug-in it pleases. This is largely because the decision to block a plug-in or not lives in the renderer -- and this, in turn, is necessitated by the click-to-play.

However, in the event that the browser determines that the status of a plug-in is "blocked" for whatever reason, we can refuse to load the plug-in at the browser side. This is only slightly complicated by the need to handle browser-mediated user authorizations (infobars, right-click menu and page action icon).

So we can become secure against compromised renderers. For example, a compromised renderer now cannot load the Java plug-in by default, unless the user has authorized a site to use Java and the attacker knows what that site is. A majority of users have Java installed yet never use Java. So we can protect those users.

## Solution

Only permit plug-in loads in the browser if the plug-in isn't blocked or the user has authorized it with a browser-mediated interaction. For example, a compromised renderer now cannot load the Java plug-in by default, unless the user

has authorized a site to use Java and the attacker knows what that site is. A majority of users have Java installed yet never use Java. So we can protect those users.

## Codes

"Execution of user-blocked plug-in"

---

## [CVE-2013-0896](#)

### Context

Plug-in execution. BrowserPluginGuest **blindly trusts the size of shared memory regions leading to overflow.**

### Problem

BrowserPluginGuest trusts the shared memory region sizes **passed in messages from renderers**. When the browser attaches to these regions it does not **sanity check** the region sizes and can be made to write beyond the end of the mapped region.

### Solution

Browser Plugin: Simplified BrowserPlugin Damage Buffer

1. Less **platform-specific code.**
2. Use base::SharedMemory instead of TransportDIB.
3. Use scoped\_ptr to simplify cleanup logic.
4. More **validity checks**

## Codes

"Perform security check on unsanitized data", "Memory corruption"

---

## [CVE-2013-0831](#)

### Context

Extensions > Loading Resources (Directory Path Traversal)

**Directory traversal vulnerability** in Google Chrome before 24.0.1312.52 allows remote attackers to have an unspecified impact by **leveraging access to an extension process.**

### Problem

I "found" this via code inspection while looking at an unrelated bug, checking for places where folks might have existing code I could borrow to prevent directory traversal escapes. Consider extension\_resource.cc:66: for (std::vector::const\_iterator i = components.begin(); i != components.end(); i++) { if (\*i == FilePath::kParentDirectory) { depth--; } else { depth++; } if (depth < 0) { return FilePath(); } } This logic **fails to account for "./" in path names**, e.g. given something like ../../.. we will be up two levels but will compute depth == 0.

### Solution

**Added a check** to enforce that it does **not escape the directory**.

## Codes

"Installer", "Data leakage", "Improper validation of manifest files"

---

## CVE-2012-5126

### Context

[Use-after-free vulnerability](#) in Google Chrome before 23.0.1271.64 allows remote attackers to cause a [denial of service](#) or possibly have unspecified other impact via vectors related to the handling of plug-in placeholders.

### Problem

[plug-in is being removed from the DOM while we're initializing it](#)

### Solution

[Set the new plug-in on the container before initializing it](#). Once the plug in is removed , destroy the old plug in

### Codes

"Object deallocation", "Use after free"

---

## CVE-2012-5125

### Context

Extensions > Deallocator

[Use-after-free vulnerability](#) in Google Chrome before 23.0.1271.64 allows remote attackers to cause a [denial of service](#) or possibly have unspecified other impact via vectors related to the handling of extension tabs.

### Problem

A [Use-After-Free that crashes the browser after the extensions is closed](#). 0. Get a Chrome instrumented with ASan (the one at goto/chrome-asan is a bit stale, but fine. The bug is also reproducible with the ToT Chrome) 1. Install the "[Screen Capture by Google](#)" extension (ID: cpngackimfmofbokmjmljamhdncknpmg) 2. Open any webpage, click on the Screen Capture icon and select "Capture Whole Page" 3. In the Screen Capture window, click the "Close" button.

### Solution

Do not access lthisl after this point. Run() ended up closing the tab that owns us. [Check that the object is still available before calling it.](#)

### Codes

"Application crash", "Object deallocation"

---

## CVE-2012-2881

### Context

It is [possible to cause webkit to fire a readyStateChange event when pdf object is removed by removing the pdf object on DOMContentLoaded event](#). Then it is possible to append the removed pdf object back to document which causes a [use after free later](#). Steps ===== 1. Download and host test3.html on local web server. 2. Open test3.html on chrome. 3. Page will display an alert box. Press escape to dismiss alert box or click ok button of alert box. 4. Page will display an alert box again. Press escape to dismiss alert box or click ok button of alert box. 5. Page will display an alert box again for third time. Press escape to dismiss alert box or click ok button of alert box. Chrome will display sad tab due to heap use after free.

### Problem

It is possible to cause webkit to fire a readyStateChange event when pdf object is removed by removing the pdf object on DOMContentLoaded event. Then it is possible to append the removed pdf object back to document which causes a use after free later.

#### Steps

=====

1. Download and host test3.html on local web server.
2. Open test3.html on chrome.
3. Page will display an alert box.  
Press escape to dismiss alert box or click ok button of alert box.
4. Page will display an alert box again.  
Press escape to dismiss alert box or click ok button of alert box.
5. Page will display an alert box again for third time.  
Press escape to dismiss alert box or click ok button of alert box.  
Chrome will display sad tab due to heap use after free.

#### Analysis of this issue

=====

1. Web page has embed tag which embeds a pdf file.
2. This embed element is removed on DOMContentLoaded event of document.
3. This causes a readyStateChange event to fire prematurely.
4. Then on readyStateChange event, removed embed element is attached to the document again. This is the cause of use after free.

#### Solution

ASSERT(!eventDispatchForbidden()) fires when removed plugin re-inserted as part of readyStateChange. Removing a plugin causes a detach which can cancel the last remaining load on a page, resulting in a readyStateChange event during a time when things are inconsistent. Defer the detach which triggers this chain of events until after the node is fully removed from the document's elementsById map.

#### Codes

"Application crash", "Use after free", "Early deallocation of plug-in objects"

---

## CVE-2012-2880

#### Context

race condition with windowless plugin buffers

#### Problem

WebPluginProxy::CreateDIBAndCanvasFromHandle() calls scoped\_ptr::reset(). This is deleting a SkCanvas subclass which apparently has a pending paint. Comments in CreateDIB...() suggest this could happen in a chain of multiple resizes. There's a Mac-only special case in Paint() using weak pointers to handle contexts changing during painting. If non-Mac code could change the canvas being used during delegate\_->Paint(), we'd be restoring stage on the wrong canvas.

#### Solution

Fix race condition with windowless plugin buffers. The problem, which is already fixed for Mac, is that the buffers can be deleted during a paint because of a resize during an NPN\_Evaluate call. So keep a local reference.

## Codes

"Application crash", "Race condition"

---

## CVE-2012-2878

### Context

**Heap-use-after-free** in WebKit::WebElement::document

m\_pluginWidget member of FrameLoaderClientImpl is **keeping the widget alive past the destruction of the document**. This **keeps the instance registered** so that a delayed GetWindowObject is **still processed, rather than just erroring upon enter**.

### Problem

The plugininstance has a raw ptr to a webplugincontentsimpl which has a raw ptr to an HTMLPluginElement from the document which no longer exists. Now, the m\_pluginWidget is **just about to be cleared** by FrameLoaderClientImpl::redirectDataToPlugin (called from PluginDocumentParser::appendBytes), but before that can happen, **layout causes the plugin to be created**, which processes a sync message, **which can catch the delayed GetWindowObject in its nested message loop**.

### Solution

**Check if pluginWidget object is alive**

## Codes

"Application crash", "Check object is not null", "Use after free"

---

## CVE-2012-2877

### Context

Extensions > Sandbox > Process Isolation > **Shutdown Chrome extensions bug cause crash in all Chrome processes**

### Problem

Chrome extensions bug cause crash in all Chrome processes This crash its most likely a security-related issue, as it is most likely caused by **jumping to an illegal address** (SEGFAULT). You can see in the example (attached) chrome crash after: xhr.open("GET", "http://api.duckduckgo.com/?q=" + search\_value + "&format=json", true); WinDbg crashes because the active\_dialog of AppModalDialogQueue is non-NULL but garbage. There is a **javascript alert open when the popup is dismissed**, and the alert dialog is **deleted just before the popup is deleted**. The **root cause is basically in the order the objects destructed**: "What's happening is that ExtensionPopup is closing itself directly when it loses focus. This seems to close the alert dialog as well (maybe because it is in the view hierarchy?). The AppModalDialog is deleted as the widget's delegate. **The ExtensionHost still isn't deleted in all this time, and won't be deleted until the ExtensionPopup is deleted**. The dialog is cancelled from within ~ExtensionHost, and that's where the boom happens."

### Solution

**Change the order of the objects destruction**, and checks that it is **not trying to destroy an already destroyed object**

## Codes

"Application crash", "Check object is not null", "Process Isolation", "Changing the order of deallocation of objects"

---

## CVE-2012-2816

## Context

Windows does not properly [isolate sandboxed processes](#), which might allow remote attackers to cause a [denial of service](#) (process interference) via unspecified vectors.

## Problem

By default, [sandboxed processes can open other sandboxed processes and manipulate them](#). Integrity levels and the restricted group [prevent reaching into unsandboxed processes](#). However, it's possible to start a renderer with privileged IPCs, open the process, and manipulate it directly. You duplicate the renderer's own process handle with DUPLICATE\_SAME\_ACCESS. Then you can do whatever you want to the process (read/write memory, CreateRemoteThread, etc.).

## Solution

This is a trick to keep the GPU out of [low-integrity processes](#). It [starts at low-integrity for UIPI to work, then drops below low-integrity after warm-up](#).

## Codes

"Unprivileged process manipulates a high-privileged process", "Privilege elevation"

---

## [CVE-2011-3956](#)

### Context

Extensions > Privileges Enforcement > Sandbox > Origin In the implementation of extensions privileges

The [extension implementation](#) in Google Chrome before 17.0.963.46 [does not properly handle sandboxed origins](#), which might [allow remote attackers to bypass the Same Origin Policy](#) via a crafted extension.

## Problem

The iframe sandbox [requires that the framed content run under the privileges of a unique origin and not the privileges of the document you downloaded from](#). But this doesn't seem to be true. Create an extension with a tabs permission, and 2 pages. The first say popup.html runs with full privileges and frames test.html in a sandbox. test.html has code to create a new tab, which should fail since test.html is running under a unique origin. But it doesn't. This is a [same-origin bypass](#).

## Solution

[Consider the origin when computing extension permissions](#) This patch [teaches the extension system to use the document's origin when computing extension permissions](#). Ideally, we'd use only the document's origin, but because app extents don't cover entire origins, we need to [also consider the document's URL](#).

## Codes

"Same-Origin Policy Bypass", "Incorrect origin check"

---

## [CVE-2011-3107](#)

### Context

[Chrome crashing](#), trying to call hasMethod at

<http://trac.webkit.org/browser/trunk/Source/WebCore/bindings/v8/V8NPOObject.cpp?rev=113111#L208>

Google Chrome before 19.0.1084.52 [does not properly implement JavaScript bindings for plug-ins](#), which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.

## Problem

The NPOObject [passed the alive check and has a valid \(or null\) hasProperty function pointer](#). However, the [hasMethod function pointer is non-null and garbage](#).

## Solution

[Added a check for NPN\\_IsAlive](#) in branches/chromium/1132/Source/WebCore/bindings/v8/NPV8Object.cpp and branches/chromium/1132/Source/WebCore/bindings/v8/V8NPOObject.cpp

## Codes

"JS Objects Isolation", "Application crash", "Check object is not null"

---

## CVE-2011-3080

### Context

[Race condition](#) in the Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168 [allows attackers to bypass intended sandbox restrictions](#) via unspecified vectors.

### Problem

[Sandbox IPC length checking race](#) The bug can be exploited to [allow for memory read and write inside the broker process](#) and as such [can be exploited to gain code execution](#), inside the broker process, leading to a [complete compromise of broker process and the users machine](#).

## Solution

[Fix race](#) in CrossCallParamsEx::CreateFromBuffer

## Codes

"IPC Service", "Sandbox escape", "Same-Origin Policy Bypass", "Data leakage"

---

## CVE-2011-3055

### Context

The browser native UI in Google Chrome before 17.0.963.83 [does not require user confirmation before an unpacked extension installation](#), which allows [user-assisted remote attackers](#) to have an unspecified impact via a crafted extension.

### Problem

"The invariant that must never be breached is: all extension installs, no matter how initiated, and whether they contain NPAPI or not, must be mediated by a browser dialog."

[No permission prompt when loading unpacked extension with NPAPI plugin.](#)

As part of the recent PinkiePie Pwnium exploit, it appears that the attacker was able to gain access to the extensions management page and get it to [load an unpacked extension with an NPAPI plugin](#) (see also bug 117715) [without generating a prompt](#). Looking at the code in UnpackedInstaller::OnLoaded, it looks like [it should generate a prompt in all cases unless the extension is disabled](#). It's unclear to me from reading the code if re-enabling the extension would still trigger the prompt, but my guess is that it doesn't. I'm not sure if this is what you were getting at, but I found what appear to be some holes. Say we have version 1 of the extension that has no plugin, and version 2 has a plugin (modifying the manifest in the same location).

This triggers a permission warning:

1. Load unpacked (version 1) from directory

2. Edit the manifest to be version 2 and include plugin section
3. Load unpacked (version 2) from directory

This doesn't trigger a permission warning:

1. Load unpacked (version 1) from directory
2. Disable
3. Edit the manifest to be version 2 and include plugin section
4. Load unpacked (version 2) from directory (it's still disabled)
5. Re-enable

Strangely, this also doesn't trigger a permission warning:

1. Load unpacked (version 1) from directory
2. Edit the manifest to be version 2 and include plugin section
3. 'Reload' the extension from chrome://extensions

## Solution

To show the prompt message in such scenario (<https://src.chromium.org/viewvc/chrome?revision=119135&view=revision>) "Prevent unnecessary prompts when unpacked extensions use chrome.permissions.request. We now record what permissions have been granted to unpacked extensions to make developing against the permissions API simpler. With this change, chrome.permissions.request will **generate the same prompts for packed and unpacked extensions**. This also fixes an issue where we were not prompting for unpacked extensions with plugins at installation time."

## Codes

"Not showing install warning dialog", "Silent install of plug-ins", "Consistent generation of install warning prompts"

---

## CVE-2011-3049

### Context

Extensions > Permissions > Malicious Extensions > Blacklist file [SIDE NOTE] There is also a side issue: "Also, I just noticed that the **blacklist is downloaded over HTTP**. That would **allow a man-in-the-middle to arbitrarily blacklist extensions**. So, I'll file a separate bug on that one." [...] "the blacklist manifest is fetched over https and includes a sha256 hash - when **we fetch the blacklist content over http we verify that the content's hash matches that**. See ExtensionUpdater::ProcessBlacklist."

### Problem

webRequest.onBeforeRequest can intercept calls to [http://www.gstatic.com/chrome/extensions/blacklist/l\\_0\\_0\\_0\\_7.txt](http://www.gstatic.com/chrome/extensions/blacklist/l_0_0_0_7.txt). Thus if an extension went rogue, Google **could add the extension to the blacklist but the extension could prevent Chrome from receiving the blacklist update**. To exploit the vulnerability, an extension has to put the following code in its background script: chrome.webRequest.onBeforeRequest.addListener(details) { var block = (details.url.indexOf("blacklist") != -1); console.log(details.url, block); return { cancel: block }; }, {urls: ["http:///\*"], ["blocking"]}; After doing so, you should see [http://www.gstatic.com/chrome/extensions/blacklist/l\\_0\\_0\\_0\\_7.txt](http://www.gstatic.com/chrome/extensions/blacklist/l_0_0_0_7.txt) true appear in the background console logs (which means the blacklist URL was successfully blocked). Basically, **the listener above executes BEFORE any Web request is performed**. Once the URL is the **blacklist it blocks the request, which prevents the update**.

## Solution

**Hide downloads of extensions blacklist from web request API**. This CL **prevents that extensions using the web request API** can prevent Chrome from updating its extensions blacklist. To do so, they added a method in the WebRequestAPI class to perform such checks:

```
139 // Returns true if the URL is sensitive and requests to this URL must not be modified/canceled by extensions, e.g. because it is targeted to the webstore
140 // to check
```

```
for updates, extension blacklisting, etc. 142 bool IsSensitiveURL(const GURL& url) { 143
bool is_webstore_gallery_url = 144 StartsWithASCII(url.spec(),
extension_urls::kGalleryBrowsePrefix, true); 145 bool is_google_com_chrome_url = 146
EndsWith(url.host(), "google.com", true) && 147 StartsWithASCII(url.path(), "/chrome",
true); 148 std::string url_without_query = 149 url.spec().substr(0,
url.spec().find_first_of('?')); 150 return is_webstore_gallery_url ||
is_google_com_chrome_url || 151 extension_urls::IsWebstoreUpdateUrl(GURL(url_without_query))
|| 152 extension_urls::IsBlacklistUpdateUrl(url); 153 }
```

## Codes

"Blacklists", "Dispatching events to unauthorized listeners", "Prevent blacklists from being updated"

---

## CVE-2011-3047

### Context

The GPU process in Google Chrome before 17.0.963.79 allows remote attackers to [execute arbitrary code or cause a denial of service \(memory corruption\) by leveraging an error in the plug-in loading mechanism.](#)

### Problem

The [plugin blocking logic wasn't being run for NaCl in prerendering.](#)

### Solution

[Fixed by moving plugin loading in prerendering after the NaCl checks.](#)

## Codes

"Memory corruption", "Loading plug-ins"

---

## CVE-2011-2853

### Context

[Use-after-free vulnerability](#) in Google Chrome before 14.0.835.163 allows remote attackers to cause a [denial of service](#) or possibly have unspecified other impact via vectors related to plug-in handling.

### Problem

At first glance it looks like no np plugin object is created or it gets deleted because of the empty swf file. Then the window is closed, and chrome tells the np plugin object to release itself (or releases the object, not sure yet).

Either way, there is [no such object, only garbage, leading to random memory access in a method call.](#) I'm not sure if it's flash specific or if any np plugin can have this problem. 1. WebKit can have torn down the window script object before getting around to tearing down the plugin, causing any attempt to release the window script object in NPP\_Destroy to reference freed memory. 2. Chromium has a special-case in WebPluginDelegateProxy::PluginDestroyed(), which avoids trying to release the window script object during teardown, by marking it invalid; the comment states that that is done after NPP\_Destroy so that NPP\_Destroy can script the window, which is clearly nonsense if WebKit has already torn it down. The first crash of the three above arises when, while we are blocked waiting for NPP\_Destroy to complete in the plugin process, the plugin sends us an IPC to release the window script object. The third crash of the three above could be referred to ajwong@, if it is easily reproducible (I haven't observed it myself). The underlying issue is that it's possible for references to a plugin element to cause it to (briefly) out-live its containing page, so that if it scripts the window object during deletion, it [may trample freed memory in the renderer.](#)

### Solution

Cope gracefully with plugin being destroyed during NPOObject Invoke or Evaluate. Cause the stub to ignore any further IPC messages, and to tear itself down the next time control returns to the message loop. The NPOObject will be released only if `Irelease_npobjectl` is true. This is used for the window script object stub in the renderer, which is freed with `NPN_DecompileObject` to avoid leaks, and so we must not try to release it. void DeleteSoon(bool release\_npobject);

## Codes

"Application crash", "Object deallocation", "Data leakage"

---

## CVE-2011-2789

### Context

Use after free in Pepper plug-in instantiation

### Problem

It's the stale instance hanging off the resource in ppapi

### Solution

Maintain a map of all resources in the resource tracker and clear instance back pointers when needed,

## Codes

"Installer", "Application crash", "Object deallocation"

---

## CVE-2011-2785

### Context

Extensions > Installer > Parsing manifest files

The extensions implementation in Google Chrome before 13.0.782.107 does not properly validate the URL for the home page, which allows remote attackers to have an unspecified impact via a crafted extension.

### Problem

Extensions manifest can have a "javascript:" url in the "homepage\_url" field. When a user opens the extensions page and clicks on the title of the extension, the homepage for that extension is opened. In this case, the JavaScript is executed in the context of the extensions page. This allows the extension to install another extension from the local file system. The PoC provided by kuzzcc tries to install a second extension that's packaged inside the first. The second extension can have any extension permissions it wants.

### Solution

While parsing the manifest files, the solution enforces that extensions do not define homepages with schemes other than valid web extents.

## Codes

"Installer", "Arbitrary code execution", "Bypass protection mechanism", "Code Injection"

---

## CVE-2011-2783

### Context

Extensions > UI > prompt user during install. Chrome does not prompt when you use the interface on chrome://extensions to load an unpacked extension that contains an NPAPI plugin.

## Problem

[Missing browser prompt when installing](#) unpacked NPAPI extensions.

[Chrome does not prompt](#) when you use the interface on chrome://extensions to load an unpacked extension that contains an NPAPI plugin. We should add the browser prompt to this case as a defense in depth measure against things like <http://crbug.com/83096>.

It seems like the fear here is that someone will XSS chrome://extensions and be able to [cause an arbitrary extension to be installed](#). This is only possible because (it appears) that javascript on chrome://extensions causes a file picker to be displayed then passes the result to C++, who trusts it. The solution is to have C++ show the file picker and never pass the path through JavaScript, not to have this weird dialog that only addresses one case

## Solution

[Show the install dialog for the initial load of an unpacked extension with plugins.](#) For that, created a new callback method at *chrome/browser/extensions/extension\_service.h*:

```
382 // Called by the backend when an unpacked extension has been loaded.  
383 void OnLoadSingleExtension(const Extension* extension);
```

Then, added a new class (*SimpleExtensionLoadPrompt*) to implement this feature (in *chrome/browser/extensions/extension\_service.cc*).

## Codes

"Not showing install warning dialog", "Silent install of plug-ins"

---

## CVE-2011-2358

### Context

[DESIGN-LEVEL] Extensions > UI > prompt user.

Google Chrome before 13.0.782.107 [does not ensure that extension installations are confirmed by a browser dialog](#), which makes it easier for remote attackers to [modify the product's functionality via a Trojan horse extension](#).

## Problem

Android had a bad security bug where you XSS on their gallery led to install on local machine. We can have the same issue on our store because we have [no client UI in that case](#). We do mitigate this issue today by forcing a user gesture. And we also force the client UI in the case of NPAPI.

There is no [client-UI-decision](#) for the web store. The decision was made to have an integrated purchase flow, where you only do one confirmation for both money and security, not two separate dialogs.

This means that an XSS results in an [install on local machine](#).

## Solution

Add a webstore install method that lets us prompt the user [before downloading](#). A while back we decided to minimize friction by showing extension/app permissions inline in the webstore, and let installs done via the private webstore API skip the regular extension installation confirmation that happens after downloading and unpacking the .crx file. We've reconsidered this and are now adding a new private install method that lets us go back to having the client display the confirmation dialog, but do it before downloading the .crx file. The webstore just needs to pass the [manifest](#) and icon, and then after downloading the .crx we [make sure the unpacked extension's manifest matches what we had prompted with](#).

## Codes

"Not showing install warning dialog", "Silent install of plug-ins"

---

## CVE-2011-1819

### Context

Malicious extensions [modifying protected chrome: URLs](#)

### Problem

A packaged app/extension [can access and modify all chrome](#): pages, read/write preferences, run chrome.send function, pass arguments directly to c++, [without required permissions, without using NPAPI plugin](#), content script or chrome.tabs.executeScript

### Solution

Added an if condition for checking that [non-component extensions can only access chrome://favicon and no other // chrome:// scheme urls](#). if (url.SchemeIs(chrome::kChromeUIScheme) && url.host() != chrome::kChromeUIFaviconHost && location() != Extension::COMPONENT) return false;

## Codes

"Privilege elevation", "Data leakage", "Code Injection", "Not enforcing permissions"

---

## CVE-2011-1815

### Context

How Chromium protect itself from malicious extension. It happens on the context of manifest files parsing.

Google Chrome before 12.0.742.91 allows remote attackers to [inject script into a tab page](#) via vectors related to extensions.

### Problem

[Bypass extensions permission](#): The "web\_url" attribute on a manifest field should not allow javascript: or chrome: URLs. For example, the two manifest files shown below can be used to bypass extensions permissions: manifest1.json ===== { "name": "test", "description": "test", "version": "1", "app": { "launch": { "web\_url": "javascript:alert('document.domain')" } } } manifest2.json ===== { "name": "test", "description": "test", "version": "1", "app": { "launch": { "web\_url": "chrome://history/" } } } In short, extensions can inject the following code through the "web\_url" parameter: - javascript:alert(document.domain) //chrome://newtab - chrome://appcache-internals/ XSS Preconditions: 1. Need to install an extension. No popups will be shown, since the manifest have nothing except web\_url. 2. Open a new tab and click on the app icon. executes in the context of chrome URLs.

### Solution

Make sure that extensions can [launch web urls with web safe schemes only](#). Developers added an if condition to enforce this.

## Codes

"Installer", "Arbitrary code execution", "Code Injection"

---

## CVE-2011-1813

### Context

There is a **stale frame** in UserScriptSlave::InjectScripts.

### Problem

The problem was that the UserScriptIdleScheduler was **relying on the FrameDetached notification** from its `_original_` RenderView, to **know when it should delete itself since the frame object was gone**. But when the frame gets reparented, the FrameDetached only gets sent to observers of the `_new_` RenderView.

### Solution

The fix is to have ExtensionHelper, which is per-RenderView, **proxy all these calls to ExtensionHelper, which is per-renderer**. ExtensionHelper then keeps the map of WebFrame->UserScriptIdleSchedulers, and notifies them of these events.

### Codes

"Application crash", "Object deallocation", "Stale pointer", "Notify deallocation events"

---

## CVE-2011-1450

### Context

Google Chrome before 11.0.696.57 does **not properly present file dialogs**, which **allows remote attackers to cause a denial of service** or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."

### Problem

When an object is destroyed, its select **file dialog is not informed to clear its listener** which can call back that destroyed object causing a potential for attacks.

### Solution

Before an object destruction, make sure that its **select dialogs are told that the object is gone** so that they **don't try to call it back**.

### Codes

"Application crash", "Check object is not null", "Object deallocation"

---

## CVE-2011-1435

### Context

Extensions leverage the chrome.tabs.captureVisibleTab to **capture images of any using a URL like "file://"**

### Problem

The tabs permission for extensions **allows an extension to capture an image** of any text file, directory, or image from the user's computer via the captureVisibleTab method. **Extensions should not be allowed to open web unsafe urls in tabs**.

Proof of Concept: 1. Download the attached extension. 2. Update the "file" variable in the popup.html file to point to a local text file on your computer (pick something fun, like your private key file). 3. Install the extension. 4. Open the extension's popup (sorry no icon). This all boils down to using the following: `chrome.tabs.create({url : "file:///home//.ssh/id_rsa"}); chrome.tabs.captureVisibleTab(null, function(d) { // Do something EVIL with 'd'. });`

### Solution

Implement **new restrictions** on tab.captureVisibleTab() method. It **checks that the tab does have "host" permissions to access files in the user's machines**: captureVisibleTab() can access some of the same information as JavaScript running on the page. Ensure the extension has host permissions. `if (!GetExtension()->CanExecuteScriptOnPage( tab_contents->GetURL(), NULL, &error_) { return false; }`

## Codes

"Data leakage", "Bypass protection mechanism", "Not enforcing permissions", "Read user's files"

---

## [CVE-2011-1124](#)

### Context

**Use-after-free vulnerability** in Google Chrome before 9.0.597.107 allows remote attackers to cause a **denial of service** or possibly have unspecified other impact via vectors related to blocked plug-ins.

### Problem

1. Install out-dated ice-tea java plugin.
2. Open attached crash.html.  
crash.html contains a applet.  
Chrome will show a info bar saying **ice-tea java plugin is out-dated**.
3. Move the mouse over java applet (Applet is not loaded at this moment, since plugin is outdated).
4. Wait about 3 seconds. crash.html will refresh itself.  
Once the page is refreshed chrome will display a sad tab.

### Solution

**Restore old title** in WebViewPlugin **only when loading the plugin**.

## Codes

"Application crash", "Use after free"

---

## [CVE-2011-1123](#)

### Context

It occurs when the extension has a NPAPI plugin and the extension has **not specified whether the NPAPI binary is public** (i.e., it omitted the "public" attribute in its manifest file).

### Problem

Take an extension with a non-public: NPAPI plugin:

```
https://chrome.google.com/extensions/detail/caehdcpeofiigpdhbabniblempncjj?hl=en "plugins": [ { "path": "plugins/npSwitchy.dll" }, { "path": "plugins/npSwitchy.so" }, { "path": "plugins/npSwitchy64.so" }, { "path": "plugins/iSwitchy.bundle" } ] Then on any public web page, you can instantiate that plugin. var o = document.createElement("OBJECT"); o.type = "application/x-mhdhejazi-switchy-1.6"; document.body.appendChild(o); o.doSomething(); // replace with something dangerous here It's supposed to be the case that in order for this to work that the extension needed to add "public": "true" to their plugin declaration in the manifest:  
http://code.google.com/chrome/extensions/npapi.html
```

### Solution

**Private extension NPAPI plugins should not be loaded by public web pages**. Fixed by adding a **check that Web pages should not be calling the PluginList directly**.

## Codes

"Not enforcing private code", "Bypass protection mechanism"

---

## CVE-2011-0779

### Context

[Loading of corrupted extension's configuration files.](#)

Google Chrome before 9.0.597.84 [does not properly handle a missing key in an extension](#), which allows remote attackers to cause a denial of service (application crash) via a crafted extension.

### Problem

VULNERABILITY DETAILS There is a [browser crash when loading a corrupted extension file](#) REPRODUCTION CASE  
1. Open the attached crx file 2. Click "continue" when prompted 3. The browser crashes The issue is that the crafted extension has an empty signature, that screws it up a memory allocation made in the code while loading the said extension. See Comment #1: We're bombing out on a zero-length allocation in SandboxedExtensionUnpacker::ValidateSignature [due to an empty signature](#). It's a really easy fix; we just need to add the following to the header validation checks we're already doing: if (header.signature\_size == 0) { ReportFailure("Key length is zero"); return false; }

### Solution

Added a check on SandboxedExtensionUnpacker::ValidateSignature to [check for an empty signature](#). In such case, an [error is returned and the loading of the extension is stopped](#).

### Codes

"Application crash", "Incorrect parsing of manifest file", "Accepting malformed manifest files"

## CVE-2011-0470

### Context

Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 [do not properly handle extensions notification](#), which allows remote attackers to cause a [denial of service \(application crash\)](#) via unspecified vectors.

### Problem

Steps ----- 1. Go to https://chrome.google.com/extensions/detail/leaabobiocgllbbfepphaknffhebpomn and install the extension - notification will be seen 2. Go to chrome://extensions and uninstall Notification demo extension 3. Exit browser Root cause: for security information, this is a race condition in window closing that can only happen at shutdown. Specifically, at shutdown the browser [stops all renderers and additionally forces all windows to close](#), then the notification code detects the renderer death and tries to close the window a second time, being unaware of the first.

### Solution

[Changed the logic](#) for capturing "window close" events in order to prevent the race condition. Listen for APP\_TERMINATING in notification ui; [close windows earlier in the process before they get clobbered](#) by browser\_shutdown leading to a potential double-close.

### Codes

"Uninstaller", "Application crash", "Race condition"

## CVE-2010-4491

### Context

When opening background.html of a malicious extension

Google Chrome before 8.0.552.215 [does not properly restrict privileged extensions](#), which allows remote attackers to cause a denial of service (memory corruption) via a crafted extension.

## Problem

[Caused by an use after free.](#) "Looks like installing an extension can cause a use after free in browser process (sandbox escape)."

## Solution

Only call WebInspector\_syncDispatch if it's actually a function. The [frame might have navigated away from the front-end page](#) (which is still weird).

```
if (!dispatchFunction->IsFunction())
return;
```

## Codes

"Installer", "Sandbox escape", "Application crash"

---

## CVE-2010-3417

### Context

When extension asks for permission

Google Chrome before 6.0.472.59 [does not prompt the user before granting access to the extension history](#), which allows attackers to [obtain potentially sensitive information](#) via unspecified vectors.

## Problem

Installing an extension with only the "history" permission does not generate a "Can access your history" warning (unlike apps with the "tabs" permission). This seems incorrect -- the history API gives even [more direct access to user history than the tabs/windows APIs do.](#) For reference, check out this extension

<https://chrome.google.com/extensions/detail/cahejgbbfgmlmjgdjlibphdjhagkp> (not mine) which has the history permission but does not generate an install warning.

## Solution

[Issue a warning](#) in the above scenario

## Codes

"Installer", "Incorrect warning of permissions", "Data leakage"

---

## CVE-2010-3250

### Context

When Webpages [attempt to load resources from extensions.](#)

Unspecified vulnerability in Google Chrome before 6.0.472.53 [allows remote attackers to enumerate the set of installed extensions](#) via unknown vectors.

## Problem

Web pages [should NOT be able to load resources](#) if there are NO content scripts from that extension on the page. We allow web pages to load resources from extensions as a feature to content scripts. However, if we know that an extension

does not have any content scripts on a page, then we **should not allow resources to be loaded from that extension**. Summary: Refactored extension privilege enumeration and implemented URLPattern comparisons. This will **allow checks on per origin extension resource access**. Added origin check when loading extension resources.

## Solution

**Refactored extension privilege enumeration and implemented URLPattern comparisons.** This will allow checks on per origin extension resource access. Added origin check when loading extension resources. Details: 1. Modify Extension::GetEffectiveHostPermissions() to return an ExtensionExtent (chrome/common/extensions/extension\_extent.h). The ExtensionExtent should contain: - All the URLPatterns from Extension::host\_permissions\_ - All the URLPatterns from all the matches from all the content scripts. The path component of these URLPatterns should be set to "/\*". - The code that is currently there does the above two steps, but instead of returning URLPatterns, it condenses the information down into just the hosts. That part is only needed by the install UI, and should move to extension\_install\_ui.cc somewhere. 2. Take a look at ExtensionInfo in chrome\_url\_request\_context.h. Add an effective\_host\_permissions field and populate it from Extension::GetEffectiveHostPermissions() similarly to how the others are done. 3. In extension\_protocols.cc, there are some other checks similar to the one you want to do in CreateExtensionURLRequestJob. Use context.effective\_host\_permissions.ContainsURL() to decide whether to block a resource load. **Note that this is only checking whether the extension being requested could run code in the page.** Checking whether the extension \_did\_run code in the page is much more complicated and would probably involve upstream changes to keep track of whether any injections had been done.

## Codes

"Data leakage", "Lack of security checks", "Not enforcing permissions", "Added origin check"

---

## CVE-2010-2110

### Context

Related to when the extensions modify a Web page's DOM tree.

Google Chrome before 5.0.375.55 **does not properly execute JavaScript code in the extension context**, which has unspecified impact and remote attack vectors.

### Problem

Summary: **Inappropriate context isolation** of the "Tabs" world and the "extensions" world. Details: If an extension causes DOM event to be fired (e.g. by modifying DOM tree, which is rather common, or explicitly calling dispatchEvent), the event listener installed by the main page will be **erroneously called in extension's context**. While actual handler code will be executed in context associated with the JS function (hence in page's world), JS wrappers for DOM objects will be retrieved from extension's world. This **allows a malicious page to mess with extension's Object.prototype by following prototype chain of any DOM object** -- e.g. by installing property getters/setters there. Data sent to/from background page may sometimes be **intercepted and extension's logic altered**. Note that the extent appears to be limited to DOM object prototypes -- the page handler still runs in page's world, and whatever code it may trick extension to execute by modifying prototypes, will **still be running in page's context**.

## Solution

**Changed its Javascript engine (V8) to check the context of the event to know where to dispatch the event:** 48 v8::Local<WorldContextHandle>::adjustedContext(V8Proxy\* proxy) const 49 { 50 if (m\_worldToUse == UseMainWorld || !m\_context || m\_context->get().IsEmpty()) 51 return proxy->mainWorldContext(); 52 53 return v8::Local<WorldContext>::New(m\_context->get()); 54 }

## Codes

"JS Objects Isolation", "Improper Objects Isolation"

---

## CVE-2010-2108

### Context

When the user blocks certain plug-ins to be executed it allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.

### Problem

Plugins are not always blocked by content settings.

In Chromium, users are allowed to select certain Websites that are authorized to load plugins into the browser. The problem in this CVE is that it allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.

Repro steps:

- 1- Modify content settings to block all plugins
- 2- Load test case
- 3- Click button
- 4- Notice that the plugin loads and can be played

The bug is likely related to the fact that we only send down the blocked content settings in response to a top-level navigation. In this example, there is no top-level navigation since the newly opened window is to about:blank.

### Solution

The key here is to realize that the newly-created window doesn't have a host, and thus no host-based settings could apply to it. And the only way for it to get a host is to navigate, at which time we'll pass the right setting for the new host. Therefore, the only settings that can apply are the global defaults. That suggests the fix: when the renderer wants to create a new view, it sends an IPC to the browser; at that time, we should pass down the default settings so the renderer can apply them to the new view. We can use our existing IPC for this. This should be a small fix so we can merge it to the branch even after the feature freeze, but if anyone wants to do it now they're welcome.

### Codes

"Execution of user-blocked plug-in", "Passing user-defined blocked plugins info to app host"

---

## CVE-2010-1229

### Context

Sandbox Infrastructure (IPC mechanism) in Google Chrome before 4.1.249.1036 does not properly use pointers, which has unspecified impact and attack vectors.

### Problem

A compromised renderer can pass an arbitrary pointer to the plugin process; this pointer is then dereferenced and manipulated (written) in the plugin process. This could be used to corrupt the plugin process and execute arbitrary code outside the sandbox.

#### ***Steps to reproduce:***

1. Create a plugin.htm page with the following (this just loads the Acrobat plugin so you can mess with it):

```
<body>
<embed id="pdf" type="application/pdf" hidden="true" width="0" height="0"></embed>
```

```

</body>
<script>
    var obj = document.getElementById("pdf");
    var x = new Object();
    obj.messageHandler = x;
</script>

```

2. Set a breakpoint in the renderer process on ParamTraits::Write()
3. Attach to the renderer process and load plugin.htm.
4. After breaking, change the value of p.type to 7 (which is NPVARIANT\_PARAM\_OBJECT\_POINTER; it should initially be 6, which is NPVARIANT\_PARAM\_OBJECT\_ROUTING\_ID).
5. Change the value of p.npobject\_pointer to 0x41414141 (or any garbage value) to trigger a crash on a write violation in the plugin process. The plugin process will read the supplied value with ParamTraits::Read() and treat it as an NPObjec pointer. The reference count (address+4 on x86) is incremented shortly after reading, which is why a crash occurs when an invalid address is provided.

#### ***Root Cause of the Problem:***

The **renderer and plugin processes can send over raw NPObjets valid in the other side's address space**. Basically, the way this works is if an NPObjec is marshaled over to the other side, an NPObjecStub is created in the caller address space and a NPObjecProxy is created on the other side. The NPObjecProxy is passed the raw NPObjec pointer which is **used as a cookie**. If the original NPObjec needs to be passed back we pass the underlying NPObjec saved in the NPObjecProxy. The receiver does not validate whether this NPObjec is **valid before invoking on it**. While this is mostly fine, in the case of a compromised renderer invalid addresses could be passed back to the plugin which would invoke on these addresses and crash.

#### **Solution**

Fix is to never **pass raw object pointers** across and just pass the corresponding **routing.id** of the NPObjecStub. The **receiver validates this object** by invoking a new method GetNPObjecListenerForRoute on the PluginChannelBase. This method returns the corresponding NPObjec listener for the routing id. We then retrieve the underlying NPObjec from the listener and use it. The map of NPObjecListeners which is maintained by PluginChannelBase has been changed to hold NPObjecBase pointers instead. NPObjecStub and NPObjecProxy implement the new NPObjecBase interface which provides methods to return the underlying NPObjec and the IPC::Channel::Listener pointer.

#### **Codes**

"IPC Service", "Passing raw pointers to plug-ins", "Sandbox escape", "Remote Code Execution"

# Firefox

---

## [CVE-2016-1966](#)

### Context

When Firefox handles [NPAPI plug-ins that create multiple objects](#) of type NPObject that [needs to be wrapped with an Object Wrapper](#).

### Problem

We believe there to be an incorrect assumption [regarding the purpose of a certain variable assignment](#) which is assumed to be obsolete. The 'entry' variable is a pointer to an entry inside the data storage of the global 'sNPObjWrappers' (which keeps track of the [object wrappers](#) used in the application). This may cause the [NPAPI subsystem to crash](#). The high-level PoC to trigger the vulnerability and cause a crash is as follows:

1. write a NPAPI plug-in which has a function that creates and returns a new NPObject every time it is called; 2. call that function in a loop from Javascript. The [browser will likely crash](#) when a HashTable Object resizes its underlying data storage."

### Solution

Fix an erroneous [nsNPObjWrapper](#) assertion.

### Codes

"Application crash", "Object wrappers"

---

## [CVE-2016-1949](#)

### Context

Mozilla Firefox before 44.0.2 [does not properly restrict the interaction between Service Workers and plugins](#), which allows remote attackers to [bypass the Same Origin Policy](#) via a crafted web site that [triggers spoofed responses](#) to requests that use NPAPI, as demonstrated by a request for a crossdomain.xml file.

### Problem

NPAPI-initiated [network requests can be intercepted by service workers](#), hence [breaking plugin origin expectations](#)

### Solution

Make plugin network requests [bypass service worker interception](#)

### Codes

"Same-Origin Policy Bypass", "Steal data", "Intercept HTTP requests"

---

## [CVE-2016-1948](#)

### Context

Mozilla Firefox before 44.0 on Android [does not ensure that HTTPS is used](#) for a lightweight-theme installation, which allows [man-in-the-middle attackers](#) to replace a theme's images and colors [by modifying the client-server data stream](#).

### Problem

To install a lightweight theme, we listen for custom events from addons.mozilla.org, and we check the document URI to [make sure these events are actually coming from addons.mozilla.org](#). However, we [don't check the scheme to ensure it's https](#). This creates the [opportunity for a malicious party to spoof the DNS entry](#) for http://evil.addons.mozilla.org/ and from there still [act with the same privileges as https://addons.mozilla.org/ and install themes](#).

## Solution

Add the [HTTPS check for schemes](#).

## Codes

"Installer", "Man-in-the-middle attack", "Spoofed origin of an install request"

---

## CVE-2015-7223

### Context

The WebExtension APIs in Mozilla Firefox before 43.0 [allow remote attackers to gain privileges](#), and [possibly obtain sensitive information or conduct cross-site scripting \(XSS\) attacks](#), via a crafted web site.

### Problem

Firefox [doesn't check that a document belongs to an extension before injecting APIs into it](#). In the case of background pages, it [continues injecting APIs into new window globals even after the first load](#). This means that if a background page navigates to a remote web page, that page has the [full privileges of the extension](#). Remote URLs loaded into popups get the [same elevation of privileges too](#).

## Solution

[Don't inject WebExtension APIs into documents without WebExtension principals](#)

## Codes

"Privilege elevation", "Steal data", "Cross-site scripting (XSS)", "Lack of security checks"

---

## CVE-2015-7196

### Context

Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4, when a [Java plugin is enabled, allow remote attackers to cause a denial of service](#) (incorrect garbage collection and application crash) or [possibly execute arbitrary code](#) via a crafted Java applet that deallocates an in-use JavaScript wrapper.

### Problem

A Java Plugin [destroys an object](#) in a thread other than the main thread, which causes its [buffer store entry not to be removed](#) in the main thread. This causes the GC to [crash](#) when it encounters the buffer store entry.

It possible result in [arbitrary code execution](#) via a crafted Java applet that deallocates an in-use JavaScript wrapper.

## Solution

[Add a MOZ\\_CRASH](#) if the thread where the object is destroyed is not the main one.

## Codes

"Application crash", "Arbitrary code execution"

---

## CVE-2015-7187

### Context

The Add-on SDK in Mozilla Firefox before 42.0 **misinterprets a "script: false" panel setting**, which makes it easier for remote attackers to conduct **cross-site scripting (XSS) attacks** via inline JavaScript code that is **executed within a third-party extension**.

## Problem

When creating extensions, if it specifies that it will not use JS (allow: { script: false }), it can **still write in-line JS code** in HTML pages which will be executed. This means that attackers can **perform XSS attacks through in-line JS in extensions**. The problem was apparently in a **default true to allow inline JS**

Steps to reproduce:

1. Create a browser extension for Firefox.

2. Create a panel with script: false:

```
function createPanel () {
    var sd = require("sdk/self").data;
    myPanel = require("sdk/panel").Panel({
        width: 640,
        height: 522,
        allow: { script: false },
        contentScriptFile: [ sd.url("full.js"), sd.url("popupscript.js") ]
```

3. Pull an external html page into the panel and include: <script>alert('this shouldnt happen');</script>

Issue was found on firefox 40, but I believe it exists prior.

Actual results:

Alert box with "this shouldnt happen" appears.

Expected results:

Inline script **should have been ignored due to this flag:**

allow: { script: false }

## Solution

**Check for the allow script specification** before running any sort of JS.

## Codes

"Cross-site scripting (XSS)", "Bypass protection mechanism"

---

## CVE-2015-4498

### Context

The add-on installation feature in Mozilla Firefox before 40.0.3 and Firefox ESR 38.x before 38.2.1 **allows remote attackers to bypass an intended user-confirmation requirement** by constructing a crafted data: URL and triggering navigation to an arbitrary http: or https: URL at a certain early point in the installation process.

## Problem

When the page is redirecting or navigating by an href link, JavaScript or server redirect, Firefox throws the '*Firefox prevented this site (site.com) from asking you to install software on your computer.*' **warning at the user**, which needs to explicitly be accepted for the add-on to continue installing.

There is, however, a simple vulnerability that lets an [attacker bypass this dialog](#), which allows a rather nasty attack on the user. Basically, there is one exception in which the dialog will not be shown, which is if the user pastes or copies the direct link/URL in the URL bar. The user could also just click on links, redirects etc that lead to this page, because a data uri redirected to the page which itself redirects with a 'page moved header' to the location of the add-on, will disrupt that 'chain' and [installation of the add-on will start without the dialog](#), as if the user typed it in directly.

## Solution

Check that the triggeringPrincipal subsumes the principal of the document loaded in the tab that started the install. The fix is to [block cross-origin add-on install requests](#).

## Codes

"Not showing install warning dialog", "Silent install of plug-ins", "Block cross-origin install requests"

---

## CVE-2015-4495

### Context

#### [PlayPreview \(PDF Viewer\)](#)

The PDF reader in Mozilla Firefox before 39.0.3, Firefox ESR 38.x before 38.1.1, and Firefox OS before 2.2 allows remote attackers to [bypass the Same Origin Policy, and read arbitrary files or gain privileges](#), via vectors involving crafted JavaScript code and a native setter, as exploited in the wild in August 2015.

### Problem

Security researcher Cody Crews reported on a way to [violate the same origin policy and inject script into a non-privileged part of the built-in PDF Viewer](#).

This exploit [allows attackers to read and copy information on victim's computer](#), once they view the web site crafted with this exploit.

Proof of Concept: Create a index.html and copy and paste the following html into it:

Test: Run the index.html (Make sure the main.js is in the same directory) and we should be able to see the directory listing.

## Solution

WIP [disables native PDF plugins](#) (In reply to Boris Zbarsky [:bz] from comment #1)

"So I tried to hack on this last night but discovered that at least on my Mac > we're treating the Adobe PDF plug-in as always disabled, which is not very > helpful for debugging.

If you can tell me how to detect the "internal PDF viewer is enabled" state,

I can try to put up some patches that implement this proposal for testing... The PDF viewer detects if it is enabled via multiple configuration flags. See <http://mxr.mozilla.org/mozilla-central/source/browser/extensions/pdfjs/content/PdfJs.jsm#275> . I think the best way to detect is PDF viewer is [enabled is to check stream converter](#). I created a WIP patch (see attachment) -- I will check if the test page works on Windows with internal PDF viewer on/off soon. Remove PlayPreview usage from PDF viewer"

## Codes

"JS Objects Isolation", "Same-Origin Policy Bypass", "Data leakage"

---

## CVE-2015-2709

### Context

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 38.0 allow remote attackers to cause a [denial of service](#) (memory corruption and application crash) or [possibly execute arbitrary code](#) via unknown vectors.

### Problem

A [missing nullptr check](#) in GetDocument and a [missing check of the content pointer before initializing](#) instanceOwner cause Firefox to [crash](#).

## Solution

[Add null check](#)

## Codes

"Application crash", "Check object is not null"

---

## CVE-2015-2706

### Context

[Race condition](#) in the AsyncPaintWaitEvent::AsyncPaintWaitEvent function in Mozilla Firefox before 37.0.2 allows remote attackers to [execute arbitrary code or cause a denial of service](#) (use-after-free) via a crafted plugin that [does not properly complete initialization](#).

### Problem

[Failed initialization of the plugins causes a race condition](#), because the [destroyer of an object linked to the plugin is not called](#), which causes the potential for UAF.

## Solution

[Destroy the owner object](#) - related to the plugin - if the plugin fails to initialize.

## Codes

"Application crash", "Object deallocation", "Race condition", "Failed initialization of the plugins", "Use after free"

---

## CVE-2015-0812

### Context

Mozilla Firefox before 37.0 [does not require an HTTPS session](#) for lightweight theme add-on installations, which allows [man-in-the-middle attackers to bypass an intended user-confirmation requirement](#) by deploying a crafted web site and [conducting a DNS spoofing attack](#) against a mozilla.org subdomain.

### Problem

Extended browser access is granted to some Mozilla-owned domains, such as addon management for addons.mozilla.org, which is defined by the default\_permissions file, as I understood it. But unlike the "UITour" permissions granted for www.mozilla.org, this [API is not restricted to the https:// protocol](#). This should not be a security risk per se, since addons.mozilla.org provides HSTS headers and is included in the static HPKP pinning list anyways, which [should render any attempt to tamper with plain HTTP traffic impossible](#). Nevertheless [sub-subdomains do not seem to enforce SSL here](#). So a MITM can [spoof the DNS entry](#) for http://evil.addons.mozilla.org/ and from there still act with the same privileges as https://addons.mozilla.org/.

## Solution

[Add the HTTPS check for schemes](#). Side note: Comment #2: "AFAIK, the only reason not to enforce that are historical - changing it may break existing legitimate 3rd party install sites. And specialized cases like enterprise environments, I guess - but I don't have any data to back that up (and we can work around that anyway). We do perform a [reasonably strict HTTPS check in the install phase, but we allow a bypass using a hash check](#). That's designed for a MitM of the actual install file, not the install request. If a MitM can control the install request site, then it would likely be pointing at a file on a site it controls anyway - so our [checks in the install phase won't help](#). I think the benefits outweigh the costs of what we may break. Saying that, needinfo on Dave in case he has more historical context around this. In the mean time, I'll work up a patch."

## Codes

"Installer", "Man-in-the-middle attack", "Spoofed origin of an install request"

---

## [CVE-2014-8643](#)

### Context

Mozilla Firefox before 35.0 on Windows allows remote attackers to **bypass** the Gecko Media Plugin (GMP) **sandbox protection** mechanism by **leveraging access to the GMP process**, as demonstrated by the OpenH264 plugin's process.

### Problem

The sandboxed plugin-container.exe process on Windows holds a handle to the parent process. While the **access rights on this handle are somewhat limited** (0x101441) it still **allows us to duplicate handles in the parent process** (PROCESS\_DUP\_HANDLE). Using DuplicateHandle we can issue a call that duplicate the process handle from the parent process to our current process (-1 a pseudo handles to the parent and current (sandboxed process). The call **will succeed and a new handle to the parent process is created in the sandboxed child**. This handle has full access to the parent which then **allows for executing arbitrary code in the parent** through CreateRemoteThread.

### Solution

**Do not allow calls to OpenProcess function**, which allows handles to be duplicated, after user content has been loaded.

### Codes

"Sandbox escape", "Unprivileged process manipulates a high-privileged process", "Privilege elevation"

---

## [CVE-2014-1519](#)

### Context

PluginModuleParent **may delete its subprocess** before calling MessageChannel::Clear, resulting in badness

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0 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.

### Problem

1) PluginModuleParent contains a PluginProcessParent, mSubprocess. When PluginModuleParent is created by static ::LoadModule, It passes parent->mSubprocess->GetChannel() to parent->Open(). [A] 2) PluginModuleParent::Open(), calls PluginModuleParent->mChannel->Open(), which is a MessageChannel. 3) MessageChannel::Open creates a ProcessLink, mLink, and passes it the channel from the subprocess in (1) [B] 4) NP\_Initialize **returns an error from the plugin**. We set mShutdown = true without actually calling NP\_Shutdown. [E] There are a few other pathways that do something similar [C] [D] (maybe [F], but the callers I checked are caused by channel shutdown) 5) We decide to destroy PluginModuleParent, and call in order: - ~PluginModuleParent - mSubprocess->Destroy() - ~MessageChannel (PluginModuleParent.mChannel destructor) - MessageChannel::Clear - delete mLink - ~ProcessLink - mTransport->set\_listener(); mTransport is the channel obtained from mSubprocess in (1) 6) mSubprocess->Destroy() queues a task on the io thread to run ldelete this!. This task then races with us getting to MessageChannel::Clear. **If it wins the race, MessageChannel.mLink now has a poisoned mTransport, and we crash.** This can be reproduced in a debugger by breaking at [G] and [E]. Fudge the plugin return code at [E]\* and stop the main thread at [G] so the iothread wins the race. Backtrace attached, which appears identical to the bug 974933 crashes: <https://crash-stats.mozilla.com/report/index/c68aee10-a11f-4191-ab54-298b12140227> \* I'm not sure about this part -- we can't call NP\_Shutdown or MessageChannel::Clear() will prevent the race. Any of the abnormal-failure paths that set lShutdown = true without calling ::Clear might be triggering this. [A] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#97> [B] <http://dxr.mozilla.org/mozilla-central/source/IPC/glue/MessageChannel.cpp#296> [C] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#1196> [D] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#111> [E] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#1228> [F] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/ipc/PluginModuleParent.cpp#731> [G] <http://dxr.mozilla.org/mozilla-central/source/dom/plugins/PluginProcessParent.cpp#82>

## Solution

**Close the channel when aborting** before successful init So mShutdown tracks if our channel has died, and the destructor calls NP\_Shutdown if it has not. This is circumvented, however, by **error paths that set it to true during init** to indicate that NP\_Shutdown shouldn't be called. All of these paths except one in LoadModule also leave the channel open erroneously, so just calling Close() when we want to shutdown without calling the plugin should fix the issue. The one case in LoadModule sets mShutdown because the object dies before calling Open(). It doesn't look like there's a sane way to assert that MessageChannel was cleaned up -- double-calling Close() is a runtime abort, and MessageChannel::Connected() **doesn't guarantee we're not somewhere between closed and connected** (and is private anyway). Is there an assertion we could add to the destructor, or is it worth modifying MessageChannel to add one? Given that this patch restores mShutdown to properly track the "After Open() before Close()" state I'm fairly confident this can't happen in other ways in the existing code at least.

## Codes

"Application crash", "Check object is not null", "Arbitrary code execution", "Memory corruption"

---

## CVE-2013-1713

### Context

In the plugin extensions (when **checking the principal** when validating URI loads of extensions )

### Problem

The InstallTrigger component can **use the wrong principal when validating URI loads**. It was happening because this component was **grabing the origin information from the outer window**. This is a potential concern in other javascript components that use the document of the window they're accessible from to perform checks against URLs before performing sensitive actions, and could also potentially be used to **bypass the same origin policy**, and other all around nastiness.

## Solution

Fix is to **get the principal information from the right context**.

## Codes

"Cross-site scripting (XSS)", "Incorrect origin check"

---

## CVE-2013-0798

### Context

Mozilla Firefox before 20.0 on Android **uses world-writable and world-readable permissions** for the app\_tmp installation directory in the local filesystem, which **allows attackers to modify add-ons before installation** via an application that leverages the time window during which app\_tmp is used.

### Problem

The installation of the Firefox for Android (FFA) makes app\_tmp **directory world readable and writable(777)**. With this configuration other applications (might be malicious) can replace any addons installed through FFA. This leads to **installing malicious addons without any awareness from users**.

## Solution

move the about:memory dumps to somewhere on /sdcard (change the tmp directory) and **set the right permissions**. Note: It's complicated in Android to change permissions for existing directories, that's why the workaround (delete the old one and create a new one with the right permissions)

## Codes

"Installer", "Extracting the plug-in to world-accessible location", "Replace benign plugins by a malicious one"

---

## [CVE-2013-0747](#)

### Context

Can [confuse PluginHandler Event](#) by listening for mutation events.

### Problem

JavaScript error: chrome://browser/content/browser.js, line 10437: iconStatus is null

```
>         let installStatus = doc.getAnonymousElementByAttribute(plugin, "class", "installStatus");
>         installStatus.setAttribute("status", "ready");
>         let iconStatus = doc.getAnonymousElementByAttribute(plugin, "class", "icon");
>         iconStatus.setAttribute("status", "ready");
```

The page [gets an event whose originalTarget is an anonymous DIV](#). It is not expected that the page be able to get a reference to the anonymous content. • Content pages shouldn't be able to access native anon content. There used to be an exception if that happened. A dedicated attacker could turn it into something pretty serious by rearranging the anonymous DOM and [clickjacking plugin install prompts](#).

### Solution

The fix was to add a <binding native="true"> attribute which would [force the pluginProblem XBL subtree to be considered native-anonymous instead of just anonymous](#), which would prevent access from content script.

### Codes

"Same-Origin Policy Bypass", "Incorrect origin check"

---

## [CVE-2012-4194](#)

### Context

[Location can be spoofed](#) using |valueOf|

### Problem

When Adobe Flash Player [checks the page location to apply the SOP \(Same-Origin Policy\)](#), it reads the return value of javascript:top.location+"\_\_flashplugin\_unique\_\_". When an object is joined with a string, its lvalueOf method is called before ItoString, and [content can redefine the former](#). This appears to have regressed in Firefox v16.0.1.

In short, the [property can be altered to gain access to attributes](#) that are not supposed to be accessed.

### Solution

Prevent [shadow of built-in location.valueOf](#).

### Codes

"JS Objects Isolation", "Cross-site scripting (XSS)"

---

## [CVE-2012-3994](#)

### Context

Using [Object.defineProperty to interfere with other add-ons](#) (or the application).

### Problem

The [Object.defineProperty can shadow ltop](#). Plugins may try to access it through *ltop.location* -- for instance, Adobe Flash Player opens javascript:top.location+"\_\_flashplugin\_unique\_\_" to determine the page origin. And it is possible to [o shadow ltop](#)

[using Object.defineProperty](#). Incidentally, Google Chrome seems to disallow redefining ltopl.

## Solution

Reload [Iframe and re-create docshell](#)

## Codes

"JS Objects Isolation"

---

## CVE-2012-3975

### Context

The created document is a data document, so it itself shouldn't load anything. [HTML parser may speculatively load something](#). (It shouldn't enable speculative loads for data documents)

### Problem

This is a bad bug in the patch for bug 102699. Before that patch, the only codepath that could lead to parsing looked like this, in order: 1) Create a document with the DOMParser's mOriginalPrincipal. 2) Call EnableXULXBL() on the document if needed 3) Call StartDocumentLoad() 4) Set the document's base URI 5) Reset the document's principal to mPrincipal. 6) Feed data into the parser. That sequence of steps was pretty clearly documented (at least in terms of the whole principal dance) and \_very\_ critical. When that bug was fixed, the XML codepath stayed as above, but HTML codepath was written more like this: 1) Create a document with the DOMParser's mOriginalPrincipal. 2) Feed data into the parser. 3) Call EnableXULXBL() on the document if needed 4) Set the document's base URI 5) Reset the document's principal to mPrincipal. But the whole point of [resetting to mPrincipal is that it MUST happen before any data goes in. Otherwise you're parsing with the system principal](#). Also, this is never calling StartDocumentLoad, so afact it's not setting up whatever state that would normally set up (e.g. the document URI) the same way as the XML path. And it's calling EnableXULXBL() too late, of course. Not like this matters much for text/html. This bug means that [using DOMParser on text/html is pretty unsafe from chrome: It allows whatever string you're parsing to poke any URI it wants](#), including ones that web content normally can't access. (On a Unix system [it allows at minimum a DoS attack by reading from file:///dev/tty](#).)

## Solution

make sure chrome [DOMParser doesn't load external resources](#)

## Codes

"Data leakage", "Trigger access to an arbitrary URL"

---

## CVE-2012-3973

### Context

The debugger in the developer-tools subsystem in Mozilla Firefox before 15.0, when [remote debugging is disabled](#), does not properly [restrict access to the remote-debugging service](#), which allows remote attackers to [execute arbitrary code by leveraging the presence of the HTTPMonitor extension and connecting to that service](#) through the HTTPMonitor port.

### Problem

If remote debugging is disabled, but HTTPMonitor is enabled, a remote user can [connect to and use the remote debug service](#).

## Solution

having the server code [take the remote-enabled flag into consideration](#) before opening the socket.

## Codes

"Data leakage", "Lack of security checks", "Bypassing restrictions on debugging remotely"

---

---

## [CVE-2012-3960](#)

### Context

During [deallocation](#)

### Problem

[Use-after-free vulnerability](#) in mozSpellChecker::SetCurrentDictionary. mozSpellChecker::SetCurrentDictionary gets called, and then mozHunspell::SetDictionary gets called (which is inlined), which in turn calls into the notification service: . The editor then catches that notification and calls nsEditor::SyncRealTimeSpell, which [can potentially lead into mInlineSpellChecker to get set to null](#), which in turn releases its mSpellChecker member , which is a mozSpellChecker which we see on the 1st frame of the freeing call stack. Then, all of this stuff returns, and when we get back to the mozSpellChecker::SetCurrentDictionary frame, \*this is dead, so any attempt to call it (such as calling Release on it) will dereference freed memory. Now, I \_think\_ that [you can't put arbitrary stuff on the stack between the time that the mozSpellChecker object dies and the time that mozSpellChecker::SetCurrentDictionary returns](#), but if I'm wrong, and you could do that, then this gives you a very nice [remote exploit](#), because the offset of Release in the vtable is pretty well known...

### Solution

Part 1: [Make sure that mozSpellChecker's refcount doesn't go down prematurely](#); Part 2: [Make sure that nsEditorSpellCheck's refcount doesn't go down prematurely](#); Part 3: [Make sure that nsEditorSpellCheck's refcount doesn't go down prematurely](#);

### Codes

"Arbitrary code execution", "Use after free"

---

## [CVE-2012-1956](#)

### Context

It occurs when [extensions manipulate the Object.defineProperty as a method to shadow the location object](#) (aka window.location)

### Problem

It is possible to [shadow the location object using Object.defineProperty](#). This could be used [to confuse the current location to plugins, allowing for possible cross-site scripting \(XSS\) attacks](#), it means that an attacker can [confuse Flash \(or other plugins\) into thinking that we're on one domain when, in reality, we're on another one](#) leading to XSS attacks.

### Solution

Create a function that does [security checks specifically for the object](#) (js::CheckDefineProperty(JSContext \*cx, HandleObject obj, HandleId id, HandleValue value, PropertyOp getter, StrictPropertyOp setter, unsigned attrs)).

### Codes

"JS Objects Isolation", "Cross-site scripting (XSS)", "Lack of security checks"

---

## [CVE-2012-0446](#)

### Context

It occurs when frame [scripts that call untrusted objects](#).

### Problem

Frame scripts [bypass XPCConnect security checks when calling untrusted objects](#). This allows for [cross-site scripting \(XSS\) attacks](#) through web pages and Firefox extensions. Frame scripts run on the special JS context for which we call

SetSecurityManagerForJSContext with flags=0, thus [if a frame script calls into an untrusted function, XPCConnect does not do proper security checks](#).

## Solution

The fix enables the [Script Security Manager \(SSM\) to force security checks on all frame scripts](#).

## Codes

"Arbitrary code execution", "Cross-site scripting (XSS)", "HTML Injection", "Inject Javascript", "Lack of security checks"

---

## [CVE-2011-3004](#)

### Context

The JSSubScriptLoader in Mozilla Firefox 4.x through 6 and SeaMonkey before 2.4 [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](#).

### Problem

When loading JS from add-ons, Firefox unwraps the wrapper objects and the code that is supposed to receive a wrapped window, it's now handed the underlying Window allowing that Window's code to [possibly catch things like expando sets and then inject its own code into the privileged call](#)

### Solution

[Use a Chrome sandbox object](#) when loading unprivileged JS code

## Codes

"Privilege elevation", "Object wrappers"

---

## [CVE-2011-3001](#)

### Context

It occurs as part of a [user-assisted attack](#). If you could convince a user to hold down the Enter key--as part of a game or test, perhaps--a [malicious page could pop up a download dialog where the held key would then activate the default Open action](#).

### Problem

For some file types this would be merely annoying (the equivalent of a pop-up) but other file types have powerful scripting capabilities. And this would provide an avenue for an attacker to exploit a vulnerability in applications not normally exposed to potentially hostile internet content. There are 2 layers of protection against an [Unauthorized installation of extensions](#): 1) The principal of the opener is checked [against whitelisted domains that are allowed to download the plugin without asking](#). If the domain is not trusted, the user [is asked to allow to download the plugin](#). 2) When the plugin is downloaded, [the user is asked to confirm the installation](#). The first protection can be circumvented by [creating a hidden "Embed" element containing an arbitrary XPI as its "pluginspage" parameter](#). The attacker can focus this element while the user holds Enter, causing a number of "Plugin Finder Service" windows to appear. The first window focuses the "Cancel" button and will just close, but all the subsequent ones will set focus on the "Manual Install" button directing to the malicious XPI. As soon as the user releases the key, the browser will start launching multiple windows with the provided URL. The windows will have a ChromeWindow object as their opener, so the user will not be asked to allow to download a plugin. The second protection can be [bypassed due to a logic error in amWebInstallListener.js](#). When no window-watcher is registered in Services, this will throw:

### Solution

It ensures that window watcher is defined, such that it can [show the install dialog](#).

## Codes

"Installer", "Silent install of plug-ins", "Arbitrary code execution", "User-assisted attack", "Bypass protection mechanism"

---

## CVE-2011-2370

### Context

Mozilla Firefox before 5.0 **does not properly enforce the whitelist** for the xpinstall functionality, which allows remote attackers to **trigger an installation dialog** for a (1) add-on or (2) theme via unspecified vectors.

### Problem

In the **install** functionality, it's **possible to redefine** window.location. Thus, content code can control this.window.location.href. Moreover, this **window is not being wrapped**.

### Solution

**Stops using the unwrapped window** and also switches to using document.documentElementObject throughout the installation process.

## Codes

"Installer", "Spoofed origin of an install request"

---

## CVE-2011-0076

### Context

**Sandbox**

Unspecified vulnerability in the Java Embedding Plugin (JEP) in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, on Mac OS X **allows remote attackers to bypass intended access restrictions** via unknown vectors.

### Problem

Vulnerability in the Java Embedding Plugin (JEP) on Mac OS X allows remote attackers to **bypass intended access restrictions** via unknown vectors.

We have discovered a vulnerability in the JEP or LiveConnect java bridge in Firefox. We initially investigated this as a bug in the Java distribution, but it now seems to be a Mozilla-specific problem. Therefore I'm giving you the proof-of-concept so that you can investigate further.  
===== javafs.html ====== ===== cut ====== 1. Put javafs.html (contents per the above) on a web server.  
2. Visit that page in Firefox. 3. Note how the script was permitted to get a reference to the java.io.FileSystem class, even though it **is declared package-local**. I reproduced the issue with Firefox 3.6.13.

### Solution

Not provided

## Codes

"Not enforcing private code", "Data leakage", "Bypass protection mechanism"

---

## CVE-2010-1585

## Context

During Plug-ins execution (protection mechanism [against unsafe javascript](#)).

## Problem

The two ns(X)HTMLParanoidFragmentSink classes are used by nsIScriptableUnescapeHTML [to sanitize \(X\)HTML by stripping attributes and tags not on a built-in whitelist](#). It allows javascript: URLs and other inline JavaScript when the embedding document is a chrome document. While there are no unsafe uses of this class in any released products, extension code could have potentially used it in an unsafe manner. [The sinks attempt to sanitize URLs by calling CheckLoadURI\[...\]DISALLOW\\_INHERIT\\_PRINCIPAL](#), but unfortunately when the target document is a chrome document (as is common with add-ons) this check allows any URI. In particular malicious href="javascript:evil()" or <iframe src="data:evil"> can slip through and create sg-critical bugs.

In short, it 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](#).

## Solution

DISALLOW\_INHERIT\_PRINCIPAL always returned "ok" for system principals. Therefore, they used a [null principal when performing the validation](#).

## Codes

"Privilege elevation", "Perform security check on unsanitized data"

---

## CVE-2010-1198

### Context

[Use-after-free vulnerability](#) allows remote attackers to [execute arbitrary code](#) via vectors involving multiple plugin instances. Deallocator A [flaw was discovered in the way plugin instances interacted](#). An attacker could potentially exploit this and [use one plugin to access freed memory from a second plugin to execute arbitrary code](#) with the [privileges of the user invoking the program](#).

### Problem

two [plugin instances could interact](#) in a way in which one plugin [gets a reference to an object owned by a second plugin](#) and continues to hold that reference after the second plugin is unloaded and its object is destroyed. In these cases, the first plugin would contain a pointer to freed memory which, if accessed, could be used by an attacker to execute arbitrary code on a victim's computer.

### Solution

instead of unwrapping an NPObj which is passed to a different instance (NPP), we should [double-wrap it](#). This means that the [other plugin would obtain a reference](#) to a nsJSObjWrapper, instead of the other-plugin-implemented NPObj\* which is destroyed when the plugin is destroyed.

## Codes

"Improper Objects Isolation", "Application crash", "Plug-in interaction"

---

## CVE-2010-0179

### Context

When [dispatching events](#) from the XMLHttpRequestSpy module (a Firebug add-on)

### Problem

When accessing this.xhrRequest.onreadystatechange, content functions (QueryInterface, getInterfaces, etc.) can be called. In other words, when add-ons try to get a reference to onreadystatechange, we call getInterfaces on the existing handler (through

the nsXPCWrappedJS). Since the application does not properly handle interaction between the [XMLHttpRequestSpy object and chrome privileged objects](#), it allows remote attackers to [execute arbitrary JavaScript](#) via a crafted HTTP response.

In short: Add-ons can get more information from calling functions they're not supposed to because [the application doesn't check for the principal](#).

## Solution

The fix is [to check the correct principal \(origin\)](#). "If no scripted code is running "above" (or called from) fp, then instead of looking at cx->globalObject, lprincipall is returned."

## Codes

"Code Injection", "Added origin check", "Incorrect origin check"

---

## CVE-2010-0177

### Context

frees the contents of the window.navigator.plugins array while a [reference to an array element is still active](#), which allows remote attackers to [execute arbitrary code or cause a denial of service](#) (application crash) via unspecified vectors, related to a "dangling pointer vulnerability." window.navigator.plugins

### Problem

error in the implementation of the window.navigator.plugins object. When a page reloads, the plugins array would [reallocate all of its members without checking for existing references to each member](#). This could result in the [deletion of objects for which valid pointers still exist](#). An attacker could use this vulnerability to [crash a victim's browser and run arbitrary code on the victim's machine](#). Successful exploitation can lead to code execution under the context of the application. This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Mozilla Firefox. User interaction is required to exploit this vulnerability in that a user must be coerced to viewing a malicious document. The specific flaw exists within the way the application implements the window.navigator.plugins array. Due to the application freeing the contents of the array while a reference to one of the elements is still being used, an attacker can utilize the free reference to call arbitrary code. Successful exploitation can lead to code execution under the context of the application. The particular vulnerability occurs within the window.navigator.plugins array. This array is implemented within dom/src/base/nsPluginArray.cpp. Each element of this array contains a reference to the mime types installed by that particular plugin. Upon page reload, the plugin array will reallocate all of its members without explicitly checking the used reference count of each member. If an attacker grabs a reference out of the array, and causes the page to reload itself, the [attacker will then have a variable that references data that has been freed by the page refresh](#).

## Solution

[detach the plugin](#) if the mimeType is not null

## Codes

"Arbitrary code execution", "Object deallocation"

---

## CVE-2010-0170

### Context

does not offer plugins the expected window.location protection mechanism, which might allow remote attackers to [bypass the Same Origin Policy and conduct cross-site scripting \(XSS\) attacks](#) via vectors that are [specific to each affected plugin Sandbox](#)

### Problem

the window.location object was made a normal overridable JavaScript object in the Firefox 3.6 browser engine (Gecko 1.9.2) because new mechanisms were developed to [enforce the same-origin policy between windows and frames](#). This object is unfortunately [also used by some plugins to determine the page origin used for access restrictions](#). A malicious page could

override this object to [fool a plugin into granting access to data on another site or the local file system](#). The behavior of older Firefox versions has been restored. we removed some code protecting the location object (on both the document and the window) because it isn't needed anymore for either web content or extensions (web pages are allowed to confuse themselves to their heart's content). In doing this, we forgot that plugins also use location.href to figure out what page they've been embedded in.

## Solution

restore the code [protecting the location object](#) that had been removed

## Codes

"JS Objects Isolation", "Same-Origin Policy Bypass", "Improper Objects Isolation"

---

## CVE-2009-2665

### Context

when certain add-ons are enabled, [does not properly handle a Link HTTP header](#), which allows remote attackers to [execute arbitrary JavaScript with chrome privileges](#) via a crafted web page, [related to an incorrect security wrapper, sandboxing](#)

### Problem

broken functionality on pages that had a Link: HTTP header when an add-on was installed which implemented a Content Policy in JavaScript, such as AdBlock Plus or NoScript. Mozilla security researcher moz\_bug\_r\_a4 demonstrated that the broken functionality was due to the window's global object receiving an [incorrect security wrapper](#) and that this issue could be used to [execute arbitrary JavaScript with chrome privileges](#).

## Solution

If we already have a wrapper at this point, it might have the wrong parent and scope, so [reparent](#) it.

## Codes

"Privilege elevation", "Arbitrary code execution", "Object wrappers"

---

## CVE-2009-1837

### Context

[Race condition](#) in the NPObjWrapper\_NewResolve function in modules/plugin/base/src/nsJSNPRuntime.cpp in xul.dll might allow remote attackers to [execute arbitrary code](#) via a page transition during Java applet loading, related to a [use-after-free vulnerability for memory associated with a destroyed Java object, deallocation](#)

### Problem

A vulnerability was reported in Mozilla Firefox. A remote user can cause [arbitrary code to be executed on the target user's system](#). A remote user can create specially crafted HTML that, when loaded by the target user, will navigate away from a web page while a Java applet is [loading to cause the applet to be deleted and then later called](#), potentially writing freed memory and executing arbitrary code on the target system. The code will run with the privileges of the target user. The vulnerability resides in NPObjWrapper\_NewResolve and [occurs when accessing the properties of an NPOObject](#). race condition in NPObjWrapper\_NewResolve when accessing the properties of a NPOObject, a wrapped JSObject. Balle and Eiram demonstrated that this condition could be reached by navigating away from a web page during the loading of a Java applet. Under such conditions the Java object would be destroyed but later called into resulting in a free memory read. An attacker could potentially [write to the freed memory before it is reused and run arbitrary code](#) on the victim's computer.

## Solution

Find out what plugin (NPP) is the owner of the object we're manipulating, and [make it own any JSObject wrappers created here](#).

## Codes

"Arbitrary code execution", "Object deallocation", "Race condition"

---

## [CVE-2009-1310](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in the MozSearch plugin implementation [allows user-assisted remote attackers to inject arbitrary web script or HTML](#) via a javascript: URI in the SearchForm element.

### Problem

[malicious MozSearch plugin could be created](#) using a javascript: URI in the SearchForm value. This URI is [used as the default landing page when an empty search is performed](#). If an attacker could get a [user to install the malicious plugin and perform an empty search](#), the SearchForm javascript: URI would be executed [within the context of the currently open page](#).

### Solution

[ignore search form urls filter](#) the SearchForm value the same way we already filter templateURI and the IconURL.

### Codes

"Arbitrary code execution", "Cross-site scripting (XSS)", "HTML Injection", "Inject Javascript"

---

## [CVE-2008-5013](#)

### Context

Mozilla Firefox Flash Player Dynamic Module Unloading Vulnerability Build identifier: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/2008020121 Firefox/2.0.0.12 the POC page runs a lot slower. The HTML content is shown, then the dialogs, but then [firefox crashes](#)

### Problem

Tipping Point has reported a bug in the Flash plugin for Firefox which they claim [contains a buffer overflow](#). This could potentially allow an attacker to [execute arbitrary code on victim's computer](#). Build identifier: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/2008020121 Firefox/2.0.0.12 the POC page runs a lot slower. The HTML content is shown, then the dialogs, but then firefox crashes

### Solution

This is a backport of the changes we took on the trunk for bug 410946. Given that our plugin initialization code is \*really\* different on the branch compared to trunk the changes to nsObjectFrame.cpp are not back-portable to the branch, but the changes to the plugin code alone seems to fix this particular problem. There's probably still fragility in the plugin frame code that is \*not\* addressed by this patch, and the only likely fix for that on the branch would be to port all the plugin loading changes from the trunk back to the branch, and that's \*really\* not trivial, and I would advice against investing in that given the \*huge\* number of regressions (and changes in functionality) we found from that change on the trunk, years after the change went in.

### Codes

"Application crash", "Arbitrary code execution"

---

## [CVE-2008-2807](#)

### Context

Faulty .properties file results in [uninitialized memory being used](#)

### Problem

I have hit a weird bug writing an extension for Firefox. The extension is localized in both french and english. One of the french \*.properties file was [not UTF-8 but ISO8859-encoded](#). The window opened by my extension retrieves 3 strings from that properties file. Surprisingly, the first retrieval (string 'textLayouts' in the attached file) did not fail, while the two others did fail. BUT what I got back from that first IGetStringFromName() call was absolutely [not what's in the properties file but some text coming from a MS Word process also running on my machine](#) !!! My XUL window was showing me a bit of the text I was editing in Word... [Fixing the encoding of the file of course resolved the issue.](#)

## Solution

Very safe fix [ensuring that the length](#) returned by `UTF8InputStream::Read` [doesn't exceed the number of characters](#) successfully converted.

## Codes

"Assuming encoding of incoming data is UTF-8", "Data leakage", "Incorrect parsing of manifest file"

---

## [CVE-2008-2806](#)

### Context

Mozilla.org distributions on the Mac that can [use Java have for some time bundled the Java Embedding Plugin](#), which allows non-WebKit browsers to use current Java versions on OS X.

### Problem

The Firefox Mac OS X Java Plugin ([MRJ Plugin](#)) is vulnerable to the ['document.domain' bypass](#). `Document.domain` gets/sets the [domain portion of the origin of the current document](#), as used by the [same origin policy](#). By using the `document.domain` exception to the same origin policy, LiveConnect, which is a feature of web browsers which allows Java applets to communicate with the JavaScript engine in the browser, and JavaScript on the web page to interact with applets, can be used [to create arbitrary socket connections](#). The code appears to use [nsIPrincipal::GetOrigin\(\)](#), [an interface to a principal, which represents a security context](#), which takes `document.domain` into account.

In short, the issue was with how the [plugin for Java applets makes calls to javascript and obtains the origin of the domains, bypassing the same origin policy](#).

## Solution

The fix was to [drop any use of GetOrigin\(\) for Java and use the principal's URI](#)

## Codes

"Same-Origin Policy Bypass", "Arbitrary code execution", "Incorrect origin check"

---

## [CVE-2008-2803](#)

### Context

When [loading scripts from extensions](#) (function: `mozIJSSubScriptLoader.LoadScript` )

### Problem

It's unsafe to use `mozIJSSubScriptLoader.loadSubScript()` with non-chrome urls or chrome urls whose scheme/host part contain uppercase characters. Scripts that are loaded in this way [do not use implicit XPCNativeWrappers when accessing content, which is used whenever privileged code is used to access unprivileged code](#). It is used to create a security wrapper that guarantees that the "native" methods/properties of an object will be called (and not the methods overridden by the webpage). As an example, Google Toolbar uses `mozIJSSubScriptLoader.loadSubScript()` with file: url, and allows an [attacker to run arbitrary code with chrome privileges](#).

## Solution

They fixed their logic for obtaining a native object wrapper. The decision of whether the subscript gets [XPCNativeWrappers or not will depend on the caller, not the file:// URI](#).

## Codes

"Object wrappers", "Not enforcing permissions"

---

## CVE-2007-3844

### Context

When [handling Privileges of plug-ins](#)

### Problem

window.open("about:blank"); or content.location = "about:blank"; or about:blank when loaded by chrome in these ways [has chrome privileges](#). This behavior could cause [security issues in certain extensions that are thinking that about:blank does not have chrome privileges](#). Imagine an extension that does: 1. Collect urls from content. 2. Load about:blank. (window.open("about:blank") or content.location = "about:blank") 3. Generate links with the urls and insert those into the about:blank document. When an user clicks a javascript: link in the generated page, the script run with chrome privileges. I'm not sure whether this should be fixed or not. If not, we need to advertise the potential problem. (There is an affected extension on AMO.)

### Solution

The three hunks of this patch do the following: 1) [Never allow chrome-privileged data:, javascript:, or about:blank loads in content docshells](#). Switch them to [inheriting principals instead](#) (which is a no-op for about:blank). This behavior is now consistent across all "normal" ways of loading, whereas before window.location allowed chrome javascript: while the nsIWebNavigation APIs, tabbrowser, and setting "src" on s did not. It's still possible to do such loads via manual invocation of nsILinkHandler, but that's not a scriptable API, and doesn't take a principal pointer anyway (it takes a node). This fixes the window.location aspect of this bug. 2) [Don't propagate a system principal as the opener principal to new content windows](#). This fixes the window.open() aspect of this bug. Note that we need both, because CreateAboutBlankContentViewer doesn't actually do a load. 3) [Remove now-redundant code in nsFrameLoader](#). The only risk here, imo is that this does change the behavior of data: and javascript: URIs loaded from chrome in content windows via window.location. If we want I can try to avoid changing that, but the code would be more complex, and I don't think we want to allow it anyway. The former is certainly not safe.

## Codes

"Privilege elevation"

---

## CVE-2006-6499

### Context

The problem is in the [JavaScript Engine](#) ( function: jsdtoa)

### Problem

When [a plugin decreases the float precision \(a global configuration\) it triggers a bug in the javascript engine](#). In short, a loop in this engine is [controlled by the floating point arithmetic](#). Since that is flawed (or rather becomes flawed after the precision is reduced ), the loop becomes infinite, and it keeps adding characters to the string until it [crashes](#). Detailed report: [Crash in jsdtoa after opening a new window](#). There is some very bad logic in jsdtoa, for the case where the double has no fractional component. File: jsdtoa.c See line 2376 /\* Do we have a "small" integer? \*/ In that case there is a loop that converts the double to a string, one digit at a time. In the loop, it looks at the most significant digit, adds that digit to the string, and then removes the digit from the double value. Then, it multiples the value by 10 so shift the digits over to the left. The problem is that [the looping logic is dependent on no floating point error being introduced](#). But, floating point error is introduced when two doubles of different magnitudes are subtracted, which is done here: 2388: d -= L\*ds; The check to exit the loop looks like this: 2410: if (!!(d \*= 10.)) break; It compares the double value to zero. Unfortunately, there is floating point error introduced, and the value of "d" never gets down to zero. Therefore, the loop becomes infinite, and we keep appending characters to the output string,

ignoring the specified size of the buffer. ( The buffer size test was done previously, based on the number of digits that it planned to place in the buffer ). My proposed fix is rather simple. Since we know up front how many digits we have to write out, we can use that number to specify the number of times that we loop, rather than depending on errorless floating point math. See the diff between the original and modified files attached. I changed the "for" line: From: `for(i = 1; ; i++) {` To: `for(i = 1; i<=k+1; i++) {` And, I removed the check on the bottom of the for loop. From: `if (!!(d *= 10.)) break;` To: `d *= 10.;` Furthermore, the logic that is there is very bad. [Description about other problem cut, will file another bug where necessary.]

## Solution

They fixed [the calculations in the loop](#). [SIDE NOTE] Even though the bug looks like a simple error logic in a loop, from what I saw in the discussions, if they had used the Chrome's approach of isolating javascript objects, this bug would never be exploited. Why? In Chrome, Javascript objects are different (each plugin has its own JS objects), this means that plugins cannot interfere with each other nor the hosting application. Thus, even if a plug-in had decreased the floating precision, the crash would not occur. So the problem seems more like not properly isolating JS objects between plugins and Thunderbird

## Codes

"Overwrite memory"

---

## CVE-2006-2784

### Context

The PLUGINSPAGE functionality in Mozilla Firefox before 1.5.0.4 allows remote user-assisted attackers to [execute privileged code by tricking a user into installing missing plugins](#) and selecting the "Manual Install" button, then using nested javascript URLs. NOTE: the manual install button is used for downloading software from a remote web site, so this issue [would not cross privilege boundaries if the user progresses to the point of installing malicious software](#) from the attacker-controlled site.

### Problem

The patch from the [previous advisory can be circumvented](#) if the following two changes are made: 1) The embed element is shown on a javascript page 2) The executed javascript accesses chrome using its full privileges to the opener object This [can be exploited using a small amount of user interaction which will likely occur given the right social engineering](#).

## Solution

Workaround Do not press the "Manual Install" button on the Firefox plugin finder. Instead use a search engine to find an appropriate plugin for the content. [moving some code in nsScriptSecurityManager.cpp.](#)

## Codes

"Installer", "Unsanitized parameter", "User-assisted attack"

---

## CVE-2005-0752

### Context

[Plug-in install](#)

The Plugin Finder Service (PFS) in Firefox before 1.0.3 allows remote attackers to [execute arbitrary code](#) via a javascript: URL in the PLUGINSPAGE attribute of an EMBED tag.

### Problem

When a webpage requires a plugin that is not installed the user can click to launch the Plugin Finder Service (PFS) to find an appropriate plugin. If the service does not have an appropriate plugin the EMBED tag is checked for a PLUGINSPAGE attribute, and if one is found the PFS dialog will contain a ["manual install"](#) button that will load the PLUGINSPAGE url.

Omar Khan reported that if the PLUGINSPAGE attribute contains a javascript: url then pressing the button could launch arbitrary code capable of [stealing local data](#) or [installing malicious code](#).

Element `embed` pluginspage attribute allows javascript urls, and somehow somebody forgot to [sanitize it](#). So can [execute arbitrary code](#).

Reproducible: Always

Steps to Reproduce:

1. Load page with an embed's pluginspage attribute set to javascript url
2. Click install missing plugins
3. Click Manual install Actual

Results: [Arbitrary code executed](#)

Expected Results: Do not execute arbitrary code.

## Solution

Do [security check when opening URL for manual plugin installation](#) A cleaner way, without security manager checks would be:

```
nsPluginInstallerWizard.prototype.loadURL = function (aUrl){
```

```
    if (window.opener.getBrowser().mCurrentBrowser)

        window.opener.getBrowser().mCurrentBrowser.contentWindow.open(aUrl);

}
```

use the current browser's contentWinow to open the url. This should be safe, thought perhaps if the current browser is pointing at an chrome:// url this could cause trouble. Probably needs more testing.

## Codes

"Arbitrary code execution", "Steal data", "Perform security check on unsanitized data"

---

## CVE-2005-0590

### Context

The underlying scenario is during an [installation](#), in which the application displays a [confirmation dialog](#) that shows a [spoofed URL](#).

### Problem

Between not checking for a [spoofed URL](#) with a username/password, and the unresizable, unwrapped [dialog for XPIinstall](#), it's possible to make a fairly convincing [spoofed URL for an XPI with InstallTrigger, due to incorrect parsing of the URL](#).

### Solution

The solution was to [strip user:pass from URL display](#). It added a function that does a preprocessing of the URL (`nsXPITriggerItem::GetSafeURLString()`).

## Codes

"Installer", "Spoofed origin of an install request", "Tricking user into installing a malicious plug-in"

---

## CVE-2005-0578

### Context

Unsafe /tmp/plugtmp directory exploitable to [erase user's files](#)

## Problem

A **predictable name is used** for the plugin temporary directory. A malicious local user could symlink this to the victim's home directory and wait for the victim to run Firefox. When Firefox shuts down the **victim's directory would be erased**. Mozilla creates the /tmp/plugtmp directory for storing plugin files, on exit, it empties this directory. A malicious local user could create a symlink at /tmp/plugtmp to a directory, when another user runs firefox the directory will be emptied. This is a **serious issue on multiuser systems**. Reproducible: Always Steps to Reproduce: 1. ln -s /home/victim /tmp/plugtmp 2. wait for victim to run and exit firefox 3. victim just lost the files in his homedir. Actual Results: Example: \$ pwd /home/taviso \$ mkdir test \$ cd test \$ for ((i=0;i<10;i++)); do touch \${RANDOM}.jpg; done \$ ls 10659.jpg 16835.jpg 26339.jpg 4062.jpg 8234.jpg 15120.jpg 22838.jpg 29316.jpg 724.jpg 9053.jpg # now malicious user wants to remove these files (i'll use user nobody for this example) \$ sudo -u nobody ln -s /home/taviso/test /tmp/plugtmp \$ ls -l /tmp/plugtmp lrwxrwxrwx 1 nobody nobody 17 Feb 6 18:43 /tmp/plugtmp -> /home/taviso/test/ # now malicious user waits until I run firefox... \$ firefox \$ ls \$ echo "arghhh, my files!" Expected Results: perhaps use a mkdtemp()-style directory instead of hardcoded /tmp/plugtmp?

## Solution

Always **create unique plugintmp directories** for each browser instance, and **only delete what was created**.

## Codes

"Extracting the plug-in to world-accessible location", "Erase user's files", "Symlink attack"

---

## CVE-2005-0232

### Context

Using Flash and the -moz-opacity filter you can get access to about:config and **make the user silently change values**

## Problem

Plugins (such as flash) can be used to **load privileged content into a frame**. Once loaded, various spoofs can be applied to **get the user to interact with the privileged content**. Michael Krax's "Fireflashing" example demonstrates that an attacker can open about:config in a frame, hide it with an opacity setting, and if the attacker can **get the victim to click at a particular spot** (design some kind of simple game) you could **toggle boolean preferences, some of which would make further attacks easier**. The "firescrolling" example demonstrates arbitrary code execution (in this case downloading a file) by convincing the user to scroll twice. Details: Using Flash and the -moz-opacity filter it is possible to display the about:config site in a hidden frame. By making the user double-click at a specific screen position (e.g. using a DHTML game) you can toggle the status of boolean config parameters. As long as the number of about:config parameters is unchanged (unlikely a casual user will change them) you can move the parameter you want to change to the specified screen position by using CSS (change the .hideframe class). Reproducible: Always Steps to Reproduce: 1. Open <http://www.mikx.de/fireflashing/> 2. Open example link (make sure Flash 7 is installed) 3. Double click on the red box Actual Results: You can silently toggle any boolean config parameter Expected Results: Security manager should prevent that a plugin can open about:config or file:/// links

## Solution

Do **security checks when loading URLs from any plugin**. This will enforce that plug-ins cannot open the about:config Webpage (that has **access to privileges configuration**) r=dveditz, but don't we need to do the same thing down in nsPluginHostImpl::PostURL ?

## Codes

"Privilege elevation", "User-assisted attack", "Bypass protection mechanism"

---

## CVE-2004-0762

### Context

During **initialization of extensions**

## Problem

If a malicious Web site can control or predict when and where a user will click, it can get them to install software. Ways in which a Website can predict user clicks:

1. A game. 1a. Make the player "pick up" items by clicking them. Measure the speed with which the player moves the mouse and clicks, and once the speed stabilizes, pop up an install dialog just before the player clicks. 1b. Force the player to click at exactly the right time: a reaction-time test, shoot the monkey, etc. 1c. Convince the player to double-click an object whose location I control. 1d. Tell the player that he has infinite ammo and can shoot by pressing or holding the 'i' button on the keyboard. Pop up an install dialog when the player runs out of ammo.

2. Pop-up hell. 2a. Make the 'x' for the pop-up ad appear just where a security dialog will appear. 2b. Make fake pop-ups out of images so you can measure the victim's reaction time, average mouse acceleration, etc. Get them on the fifth "pop-up".

## Solution

They enumerated three possible alternatives, and decided to implement the following:

B) Add a one-second delay between when the dialog gets focus and when the Install/OK button becomes enabled. I say "gets focus" rather than "appears" because a site could hide an install dialog as a modal dialog of a background window for a minute and then bring the dialog to the front at a convenient time by closing the window in front.

The other alternatives were (but they're not implemented):

A) When a site tries to install software or calls enablePrivilege, display a status bar message, "This page would like to install software on your computer". Only display the dialog after the user clicks the status bar message. (Err, how do you click a status bar message with the keyboard?) C) If the total time to decide to install and download the xpi are less than five seconds, stall installation (with the "downloading..." dialog still up) until five seconds are up so the user has an extra chance to cancel. I'm worried that users might not know to cancel because they do not realize that they accidentally clicked "install" in a dangerous dialog.

## Codes

"Installer", "Not showing install warning dialog", "Silent install of plug-ins", "User-assisted attack"

## CVE-2017-15714

### Context

It occurs in the [BIRT plug-in](#), in the code that is used to Map Java attributes to Javascript constants.

### Problem

The BIRT plugin in Apache OFBiz [does not escape user input](#) property passed. This allows for [code injection](#) by passing that code through the URL. For example by appending this code "\_\_format=%27;alert(%27xss%27)" to the URL an alert window would execute.

### Solution

Fix is to [enforce html encoding of request-strings](#) passed to birt. This is done by invoking (which escapes HTML characters)

```
htmlEncode(ParameterAccessor.getFormat(request))
```

### Codes

"Unsanitized data", "Code Injection"

## CVE-2017-12796

### Context

[Deserialization of XML input](#) into objects

### Problem

Exploitation of this vulnerability is possible through a single HTTP POST request to the page at <http://localhost/openmrs/admin/reports/reportSchemaXml.form>. Accessing this page through a browser [without authenticating first](#) will redirect the user to the login page (so far so good). Under the hood, however, the application is actually executing server-side code before the HTTP redirect response is generated (not so good). Through a Java debugger, with a few strategically placed breakpoints, it becomes apparent that [a validation function is being called prior to any auth checks in the reportSchemaXml form controller](#). By itself, this is a relatively low-severity issue. The end result is still a HTTP 302 to the login page. The real problem here is revealed by stepping into the call to `reportService.getReportSchema(rsx)`. Within this function, a deserialization call can clearly be observed. Furthermore, this [deserialization call takes as input user-provided data from the original POST request](#). Again, this is a pre-auth POST request; no [authentication checks have been run](#). An additional step into the `deserialize()` function shows that XStream is being used for deserialization instead of builtin Java deserialization fuctions. At this point it has been established that the [application is deserializing arbitrary input from an unauthenticated user without any filtering](#). For a full explanation of why this is so bad, and why this will almost certainly lead to some kind of [RCE](#) vulnerability, check out this article by FoxGlove Security. The next step in the exploitation process is to [craft a malicious Java object that, when passed to the XStream deserialize\(\) function, will result in RCE](#).

### Solution

[Validation of the XML input](#) before deserialization. This avoids that a plug-in [injects OS commands](#).

### Codes

"Arbitrary code execution", "Perform security check on unsanitized data", "Code Injection"

## CVE-2014-3694

### Context

Plug-ins: GnuTLS SSL/TLS and OpenSSL SSL/TLS plugin. It occurs **during the handling of X.509 certificates from SSL servers**.

### Problem

Both of libpurple's bundled SSL/TLS plugins (one for GnuTLS and one for NSS) **failed to check that the Basic Constraints extension allowed intermediate certificates to act as CAs**. This **allowed anyone with any valid certificate to create a fake certificate** for any arbitrary domain and Pidgin would trust it.

### Solution

Both bundled plugins were changed **to check the Basic Constraints extension on all intermediate CA certificates**.

### Codes

"Not checking for proper certificate validation", "Spoofing"

---

## CVE-2013-6483

### Context

XMPP protocol plugin (when handling **spoofed replies**)

### Problem

The XMPP protocol plugin **failed to ensure that iq (Instant Messaging Intelligence Quotient) replies came from the person they were sent to**. A remote user could send a **spoofed iq reply** and attempt to guess the iq id. This could allow an attacker **to inject fake data or trigger a null pointer dereference**.

### Solution

**Keep track of the 'to' when sending an iq stanza** and **make sure replies for a given stanza ID come from the same address it was sent to**.

### Codes

"Application crash", "Spoofing", "Incorrect origin check", "Inject fake data"

---

## CVE-2013-0271

### Context

MXit protocol plugin in libpurple (when handling **invalid file paths**)

### Problem

The MXit protocol plugin saves an image to local disk using a **filename** that could potentially be **partially specified by the IM server** or by **a remote user**, which could be used to **create malicious files or overwrite files of the user**.

### Solution

**Escape values** that come from the network before using them in filenames.

### Codes

"File path traversal", "Overwrite files"

## CVE-2012-6152

### Context

Yahoo! protocol plugin in libpurple (during **validation of incoming strings**)

### Problem

Many places in the Yahoo! protocol plugin **assumed incoming strings were UTF-8** and **failed to transcode from non-UTF-8 encodings**. This can lead to a **crash when receiving strings that aren't UTF-8**.

### Solution

Depending on the context, either **validate that a string is UTF-8** or **transcode the string from the appropriate encoding to UTF-8**.

### Codes

"Application crash", "Unsanitized data", "Assuming encoding of incoming data is UTF-8"

---

## CVE-2012-1178

### Context

A flaw was found in the way the Pidgin MSN protocol plug-in **processed text that was not encoded in UTF-8**. A remote attacker could use this flaw to **crash Pidgin** by sending a specially-crafted MSN message.

### Problem

In some situations the **MSN server sends text that isn't UTF-8 encoded**, and Pidgin **fails to verify the text's encoding**. In some cases this can lead to a **crash** when attempting to display the text.

### Solution

**Verify that incoming text is UTF-8**, and **sanitize** if it's not.

### Codes

"Application crash", "Sanitizing data", "Assuming encoding of incoming data is UTF-8"

---

## CVE-2011-4603

### Context

SILC protocol plugin in libpurple during **validation of incoming messages**.

### Problem

When receiving various incoming messages, the SILC protocol plugin **failed to validate that a piece of text was UTF-8**. In some cases invalid UTF-8 data would lead to a **crash**. This vulnerability is similar to CVE-2011-3594, but occurs in a different piece of code and was fixed at a later date.

### Solution

**Validate incoming strings as UTF-8** before using them as such.

### Codes

"Application crash", "Perform security check on unsanitized data", "Assuming encoding of incoming data is UTF-8"

---

## CVE-2011-4601

### Context

Oscar protocol plugin in libpurple **during validation of incoming messages**.

## Problem

When receiving various messages related to requesting or receiving authorization for adding a buddy to a buddy list, the oscar protocol plugin **failed to validate that a piece of text was UTF-8**. In some cases invalid UTF-8 data would lead to a **crash**.

## Solution

**Validate incoming strings as UTF-8** before using them as such.

## Codes

"Application crash", "Sanitizing data", "Assuming encoding of incoming data is UTF-8"

---

## CVE-2011-3594

### Context

SILC protocol plug-in when **handling non-UTF8 strings** using the glib2.

## Problem

When receiving various incoming messages, the SILC protocol plugin **failed to validate that a piece of text was UTF-8**. In some cases invalid UTF-8 data would lead to a **crash**. A flaw was reported [1] in libpurple's SILC protocol plugin, and all software which uses SILC via libpurple. The `g_markup_escape_text()` function, when called on strings that **have not been verified as valid UTF-8**, will read past the end of the string and eventually **segfault** for certain sequences in some versions of Glib2. The behaviour of this function was undefined, and because it depends on the particular version of Glib2 in use, it is unknown what the complete ramifications of the flaw is, however it has been verified that an untrusted user could **remotely crash a libpurple** client via specially crafted SILC messages. The crash is **caused by passing "user-controlled" non-UTF8 string** to the `g_markup_escape_text` function. A non-utf8 string passed to `g_markup_escape_text` causes the same string to be passed along to `append_escaped_text` in `gmarkup.c` `append_escaped_text` is supposed to parse this text and uses `g_utf8_next_char` to read the entire input string (assuming that it is utf8 of-course). `g_utf8_next_char` returns invalid pointers which causes "while (`p != end`)" loop in `append_escaped_text` to never exit. This ultimately causes OOB read and eventual **client crash**.

## Solution

**Validate incoming strings as UTF-8** before using them as such.

## Codes

"Application crash", "Assuming encoding of incoming data is UTF-8"

---

## CVE-2011-2943

### Context

IRC protocol plug-in when **processing invalid nicknames**

## Problem

**A NULL pointer dereference** flaw was found in the way IRC protocol plug-in of the Pidgin multiprotocol instant messaging client processed certain nick names, when list set of users (/who command) was issued upon user session startup and connecting user has had certain **encoding configuration** setup. A remote attacker could use a specially-crafted string as their nickname to cause the Pidgin client on the side of the victim (connecting user) **to crash**.

**Certain characters in the nicknames of IRC users can trigger a null pointer dereference** in the IRC protocol plugin's handling of responses to WHO requests. This can cause a crash on some operating systems. Clients based on libpurple 2.8.0 through 2.9.0 are affected.

## Solution

Change libpurple to **validate the data it receives from the server** before attempting to use it.

## Codes

"Application crash", "Check object is not null", "Perform security check on unsanitized data"

---

## Context

Pidgin-knotify plug-in flaw when [processing incoming messages](#)

## Problem

pidgin-knotify is a pidgin plugin that displays received messages and other notices from pidgin as KDE notifications. It uses system() to invoke ktdialog and [passes the unescaped messages as command line arguments](#). An attacker could use this to [inject arbitrary commands](#) by sending a prepared message via any protocol supported by pidgin to the victim.

*Reproducible:* Always

*Steps to Reproduce:*

1. Install and enable pidgin-knotify
2. Receive a message like ';touch /tmp/vulnerable;'
3. Confirm that /tmp/vulnerable exists

*Actual Results:* /tmp/vulnerable exists

*Expected Results:* The touch command should not be run.

The vulnerable system() call is located in src/pidgin-knotify.c, line 71-74: command = g\_strdup\_printf("kdialog --title '%s' --passivepopup "%s' %d", title, body, timeout); [...] result = system(command);

## Solution

Instead of using system(), functions of the [exec family should be used](#), e.g. [execve with a sanitized environment](#). If a dbus interface for showing notifications in KDE exists, it could be used as well. I've written a patch some time ago to remove system() and instead use dbus, and upstream has given me access to the repository so I was planning to release a new version with that when RL shit happened and all my free time went to hell

## Codes

"Arbitrary code execution", "Unsanitized data"

---

# CVE-2010-0013

## Context

MSN protocol plugin in libpurple when [processing emoticon messages](#)

## Problem

[Directory traversal](#) vulnerability in slp.c in the MSN protocol plugin in libpurple in Pidgin 2.6.4 and Adium 1.3.8 allows remote attackers to [read arbitrary files](#) via a .. (dot dot) in an application/x-msnmsgrp2p MSN emoticon (aka custom smiley) request, a related issue to CVE-2004-0122.

*NOTE: it could be argued that this is resultant from a vulnerability in which an emoticon download request is processed even without a preceding text/x-mms-emoticon message that announced availability of the emoticon.*

## Solution

[Remove ~/.purple/custom\\_smiley/ directory if it exists](#). The directory is not created by default and is created when first custom smiley is defined.

## Codes

"File path traversal", "Data leakage"

# Thunderbird

---

## CVE-2016-1966

### Context

When Firefox handles [NPAPI plug-ins that create multiple objects](#) of type NPObject that [needs to be wrapped with an Object Wrapper](#).

### Problem

We believe there to be an incorrect assumption [regarding the purpose of a certain variable assignment](#) which is assumed to be obsolete. The 'entry' variable is a pointer to an entry inside the data storage of the global 'sNPObjWrappers' (which keeps track of the [object wrappers](#) used in the application). This may cause the [NPAPI subsystem to crash](#). The high-level PoC to trigger the vulnerability and cause a crash is as follows:

1. write a NPAPI plug-in which has a function that creates and returns a new NPObject every time it is called; 2. call that function in a loop from Javascript. The [browser will likely crash](#) when a HashTable Object resizes its underlying data storage."

### Solution

Fix an erroneous [nsNPObjWrapper](#) assertion.

### Codes

"Application crash", "Object wrappers"

---

## CVE-2013-1713

### Context

In the plugin extensions (when [checking the principal](#) when validating URI loads of extensions )

### Problem

The InstallTrigger component can [use the wrong principal when validating URI loads](#). It was happening because this component was [grabing the origin information from the outer window](#). This is a potential concern in other javascript components that use the document of the window they're accessible from to perform checks against URLs before performing sensitive actions, and could also potentially be used to [bypass the same origin policy](#), and other all around nastiness.

### Solution

Fix is to [get the principal information from the right context](#).

### Codes

"Cross-site scripting (XSS)", "Incorrect origin check"

---

## CVE-2013-0747

### Context

Can [confuse PluginHandler Event](#) by listening for mutation events.

### Problem

JavaScript error: chrome://browser/content/browser.js, line 10437: iconStatus is null

```
>         let installStatus = doc.getAnonymousElementByAttribute(plugin, "class", "installStatus");
>         installStatus.setAttribute("status", "ready");
```

```
>         let iconStatus = doc.getAnonymousElementByAttribute(plugin, "class", "icon");
>         iconStatus.setAttribute("status", "ready");
```

The page [gets an event whose originalTarget is an anonymous DIV](#). It is not expected that the page be able to get a reference to the anonymous content. • Content pages shouldn't be able to access native anon content. There used to be an exception if that happened. A dedicated attacker could turn it into something pretty serious by rearranging the anonymous DOM and [clickjacking plugin install prompts](#).

## Solution

The fix was to add a `<binding native="true">` attribute which would [force the pluginProblem XBL subtree to be considered native-anonymous instead of just anonymous](#), which would prevent access from content script.

## Codes

"Same-Origin Policy Bypass", "Incorrect origin check"

---

## CVE-2012-4194

### Context

[Location can be spoofed](#) using `|valueOf|`

### Problem

When Adobe Flash Player [checks the page location to apply the SOP \(Same-Origin Policy\)](#), it reads the return value of `javascript:top.location+"__flashplugin_unique__"`. When an object is joined with a string, its `lvalueOf` method is called before `toString()`, and [content can redefine the former](#). This appears to have regressed in Firefox v16.0.1.

In short, the [property can be altered to gain access to attributes](#) that are not supposed to be accessed.

## Solution

Prevent [shadow of built-in location.valueOf](#).

## Codes

"JS Objects Isolation", "Cross-site scripting (XSS)"

---

## CVE-2012-3994

### Context

Using [Object.defineProperty to interfere with other add-ons](#) (or the application).

### Problem

The [Object.defineProperty can shadow ltop!](#). Plugins may try to access it through `ltop.location` -- for instance, Adobe Flash Player opens `javascript:top.location+"__flashplugin_unique__"` to determine the page origin. And it is possible to [shadow ltop! using Object.defineProperty](#). Incidentally, Google Chrome seems to disallow redefining `ltop`.

## Solution

Reload [Iframe and re-create docshell](#)

## Codes

"JS Objects Isolation"

---

## CVE-2012-3975

### Context

The created document is a data document, so it itself shouldn't load anything. [HTML parser may speculatively load something](#).  
(It shouldn't enable speculative loads for data documents)

## Problem

This is a bad bug in the patch for bug 102699. Before that patch, the only codepath that could lead to parsing looked like this, in order: 1) Create a document with the DOMParser's mOriginalPrincipal. 2) Call EnableXULXBL() on the document if needed 3) Call StartDocumentLoad() 4) Set the document's base URI 5) Reset the document's principal to mPrincipal. 6) Feed data into the parser. That sequence of steps was pretty clearly documented (at least in terms of the whole principal dance) and \_very\_ critical. When that bug was fixed, the XML codepath stayed as above, but HTML codepath was written more like this: 1) Create a document with the DOMParser's mOriginalPrincipal. 2) Feed data into the parser. 3) Call EnableXULXBL() on the document if needed 4) Set the document's base URI 5) Reset the document's principal to mPrincipal. But the whole point of [resetting to mPrincipal is that it MUST happen before any data goes in. Otherwise you're parsing with the system principal](#). Also, this is never calling StartDocumentLoad, so afaict it's not setting up whatever state that would normally set up (e.g. the document URI) the same way as the XML path. And it's calling EnableXULXBL() too late, of course. Not like this matters much for text/html. This bug means that [using DOMParser on text/html is pretty unsafe from chrome: It allows whatever string you're parsing to poke any URI it wants](#), including ones that web content normally can't access. (On a Unix system [it allows at minimum a DoS attack by reading from file:///dev/tty](#).)

## Solution

make sure chrome [DOMParser doesn't load external resources](#)

## Codes

"Data leakage", "Trigger access to an arbitrary URL"

---

## CVE-2012-3960

### Context

During [deallocation](#)

### Problem

[Use-after-free vulnerability](#) in mozSpellChecker::SetCurrentDictionary. mozSpellChecker::SetCurrentDictionary gets called, and then mozHunspell::SetDictionary gets called (which is inlined), which in turn calls into the notification service: . The editor then catches that notification and calls nsEditor::SyncRealTimeSpell, which [can potentially lead into mInlineSpellChecker to get set to null](#), which in turn releases its mSpellChecker member , which is a mozSpellChecker which we see on the 1st frame of the freeing call stack. Then, all of this stuff returns, and when we get back to the mozSpellChecker::SetCurrentDictionary frame, \*this is dead, so any attempt to call it (such as calling Release on it) will dereference freed memory. Now, I \_think\_ that [you can't put arbitrary stuff on the stack between the time that the mozSpellChecker object dies and the time that mozSpellChecker::SetCurrentDictionary returns](#), but if I'm wrong, and you could do that, then this gives you a very nice [remote exploit](#), because the offset of Release in the vtable is pretty well known...

## Solution

Part 1: [Make sure that mozSpellChecker's refcount doesn't go down prematurely](#); Part 2: [Make sure that nsEditorSpellCheck's refcount doesn't go down prematurely](#); Part 3: [Make sure that nsEditorSpellCheck's refcount doesn't go down prematurely](#);

## Codes

"Arbitrary code execution", "Use after free"

---

## CVE-2012-1956

### Context

It occurs when [extensions manipulate the Object.defineProperty as a method to shadow the location object](#) (aka window.location)

### Problem

It is possible to [shadow the location object using Object.defineProperty](#). This could be used [to confuse the current location to plugins, allowing for possible cross-site scripting \(XSS\) attacks](#), it means that an attacker can [confuse Flash \(or other plugins\) into thinking that we're on one domain when, in reality, we're on another one](#) leading to XSS attacks.

### Solution

Create a function that does [security checks specifically for the object](#) (js::CheckDefineProperty(JSContext \*cx, HandleObject obj, HandleId id, HandleValue value, PropertyOp getter, StrictPropertyOp setter, unsigned attrs)).

### Codes

"JS Objects Isolation", "Cross-site scripting (XSS)", "Lack of security checks"

---

## CVE-2012-0446

### Context

It occurs when frame [scripts that call untrusted objects](#).

### Problem

Frame scripts [bypass XPCConnect security checks when calling untrusted objects](#). This allows for [cross-site scripting \(XSS\) attacks](#) through web pages and Firefox extensions. Frame scripts run on the special JS context for which we call SetSecurityManagerForJSContext with flags=0, thus [if a frame script calls into an untrusted function, XPCConnect does not do proper security checks](#).

### Solution

The fix enables the [Script Security Manager \(SSM\) to force security checks on all frame scripts](#).

### Codes

"Arbitrary code execution", "Cross-site scripting (XSS)", "HTML Injection", "Inject Javascript", "Lack of security checks"

---

## CVE-2011-3001

### Context

It occurs as part of a [user-assisted attack](#). If you could convince a user to hold down the Enter key--as part of a game or test, perhaps--a [malicious page could pop up a download dialog where the held key would then activate the default Open action](#).

### Problem

For some file types this would be merely annoying (the equivalent of a pop-up) but other file types have powerful scripting capabilities. And this would provide an avenue for an attacker to exploit a vulnerability in applications not normally exposed to potentially hostile internet content. There are 2 layers of protection against an [Unauthorized installation of extensions](#): 1) The principal of the opener is checked [against whitelisted domains that are allowed to download the plugin without asking](#). If the domain is not trusted, the user [is asked to allow to download the plugin](#). 2) When the plugin is downloaded, [the user is asked to confirm the installation](#). The first protection can be circumvented by [creating a hidden "Embed" element containing an arbitrary XPI as its "pluginspage" parameter](#). The attacker can focus this element while the user holds Enter, causing a number of "Plugin Finder Service" windows to appear. The first window focuses the "Cancel" button and will just close, but all the subsequent ones will set focus on the "Manual Install" button directing to the malicious XPI. As soon as the user releases the key, the browser will start launching multiple windows with the provided URL. The windows will have a ChromeWindow object as their opener, so the user will not be asked to allow to download a plugin. The second protection can be [bypassed due to a logic error in amWebInstallListener.js](#). When no window-watcher is registered in Services, this will throw:

## Solution

It ensures that window watcher is defined, such that it can [show the install dialog](#).

## Codes

"Installer", "Silent install of plug-ins", "Arbitrary code execution", "User-assisted attack", "Bypass protection mechanism"

---

## CVE-2010-1585

### Context

During Plug-ins execution (protection mechanism [against unsafe javascript](#)).

### Problem

The two ns(X)HTMLParanoidFragmentSink classes are used by nsIScriptableUnescapeHTML [to sanitize \(X\)HTML by stripping attributes and tags not on a built-in whitelist](#). It allows javascript: URLs and other inline JavaScript when the embedding document is a chrome document. While there are no unsafe uses of this class in any released products, extension code could have potentially used it in an unsafe manner. [The sinks attempt to sanitize URLs by calling CheckLoadURI\[...\]DISALLOW\\_INHERIT\\_PRINCIPAL](#), but unfortunately when the target document is a chrome document (as is common with add-ons) this check allows any URI. In particular malicious href="javascript:evil()" or <iframe src="data:evil"> can slip through and create sg-critical bugs.

In short, it 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](#).

## Solution

DISALLOW\_INHERIT\_PRINCIPAL always returned "ok" for system principals. Therefore, they used a [null principal when performing the validation](#).

## Codes

"Privilege elevation", "Perform security check on unsanitized data"

---

## CVE-2010-0179

### Context

When [dispatching events](#) from the XMLHttpRequestSpy module (a Firebug add-on)

### Problem

When accessing this.xhrRequest.onreadystatechange, content functions (QueryInterface, getInterfaces, etc.) can be called. In other words, when add-ons try to get a reference to onreadystatechange, we call getInterfaces on the existing handler (through the nsXPCWrappedJS). Since the application does not properly handle interaction between the [XMLHttpRequestSpy object and chrome privileged objects](#), it allows remote attackers to [execute arbitrary JavaScript](#) via a crafted HTTP response.

In short: Add-ons can get more information from calling functions they're not supposed to because [the application doesn't check for the principal](#).

## Solution

The fix is [to check the correct principal \(origin\)](#). "If no scripted code is running "above" (or called from) fp, then instead of looking at cx->globalObject, lprincipal is returned."

## Codes

"Code Injection", "Added origin check", "Incorrect origin check"

---

## CVE-2008-2806

### Context

Mozilla.org distributions on the Mac that can [use Java have for some time bundled the Java Embedding Plugin](#), which allows non-WebKit browsers to use current Java versions on OS X.

### Problem

The Firefox Mac OS X Java Plugin ([MRJ Plugin](#)) is vulnerable to the '[document.domain' bypass](#)'. Document.domain gets/sets the [domain portion of the origin of the current document](#), as used by the [same origin policy](#). By using the document.domain exception to the same origin policy, LiveConnect, which is a feature of web browsers which allows Java applets to communicate with the JavaScript engine in the browser, and JavaScript on the web page to interact with applets, can be used [to create arbitrary socket connections](#). The code appears to use [nsIPrincipal::GetOrigin\(\)](#), [an interface to a principal, which represents a security context](#), which takes document.domain into account.

In short, the issue was with how the [plugin for Java applets makes calls to javascript and obtains the origin of the domains, bypassing the same origin policy](#).

### Solution

The fix was to [drop any use of GetOrigin\(\) for Java and use the principal's URI!](#)

### Codes

"Same-Origin Policy Bypass", "Arbitrary code execution", "Incorrect origin check"

---

## CVE-2008-2803

### Context

When [loading scripts from extensions](#) (function: mozIJSSubScriptLoader.LoadScript )

### Problem

It's unsafe to use mozIJSSubScriptLoader.loadSubScript() with non-chrome urls or chrome urls whose scheme/host part contain uppercase characters. Scripts that are loaded in this way [do not use implicit XPCNativeWrappers when accessing content, which is used whenever privileged code is used to access unprivileged code](#). It is used to create a security wrapper that guarantees that the "native" methods/properties of an object will be called (and not the methods overridden by the webpage). As an example, Google Toolbar uses mozIJSSubScriptLoader.loadSubScript() with file: url, and allows an [attacker to run arbitrary code with chrome privileges](#).

### Solution

They fixed their logic for obtaining a native object wrapper. The decision of whether the subscript gets [XPCNativeWrappers or not will depend on the caller, not the file:// URI](#).

### Codes

"Object wrappers", "Not enforcing permissions"

---

## CVE-2007-3844

### Context

When [handling Privileges of plug-ins](#)

### Problem

window.open("about:blank"); or content.location = "about:blank"; or about:blank when loaded by chrome in these ways [has chrome privileges](#). This behavior could cause [security issues in certain extensions that are thinking that about:blank does not have chrome privileges](#). Imagine an extension that does: 1. Collect urls from content. 2. Load about:blank.

(window.open("about:blank") or content.location = "about:blank") 3. Generate links with the urls and insert those into the about:blank document. When an user clicks a javascript: link in the generated page, the script run with chrome privileges. I'm not sure whether this should be fixed or not. If not, we need to advertise the potential problem. (There is an affected extension on AMO.)

## Solution

The three hunks of this patch do the following: 1) [Never allow chrome-privileged data:, javascript:, or about:blank loads in content docshell](#). Switch them to [inheriting principals instead](#) (which is a no-op for about:blank). This behavior is now consistent across all "normal" ways of loading, whereas before window.location allowed chrome javascript: while the nsIWebNavigation APIs, tabbrowser, and setting "src" on s did not. It's still possible to do such loads via manual invocation of nsILinkHandler, but that's not a scriptable API, and doesn't take a principal pointer anyway (it takes a node). This fixes the window.location aspect of this bug. 2) [Don't propagate a system principal as the opener principal to new content windows](#). This fixes the window.open() aspect of this bug. Note that we need both, because CreateAboutBlankContentViewer doesn't actually do a load. 3) [Remove now-redundant code in nsFrameLoader](#). The only risk here, imo is that this does change the behavior of data: and javascript: URIs loaded from chrome in content windows via window.location. If we want I can try to avoid changing that, but the code would be more complex, and I don't think we want to allow it anyway. The former is certainly not safe.

## Codes

"Privilege elevation"

---

## CVE-2006-6499

### Context

The problem is in the [JavaScript Engine](#) ( function: jsdtoa)

### Problem

When [a plugin decreases the float precision \(a global configuration\) it triggers a bug in the javascript engine](#). In short, a loop in this engine is [controlled by the floating point arithmetic](#). Since that is flawed (or rather becomes flawed after the precision is reduced ), the loop becomes infinite, and it keeps adding characters to the string until it [crashes](#). Detailed report: [Crash in jsdtoa after opening a new window](#). There is some very bad logic in jsdtoa, for the case where the double has no fractional component. File: jsdtoa.c See line 2376 /\* Do we have a "small" integer? \*/ In that case there is a loop that converts the double to a string, one digit at a time. In the loop, it looks at the most significant digit, adds that digit to the string, and then removes the digit from the double value. Then, it multiples the value by 10 so shift the digits over to the left. The problem is that [the looping logic is dependent on no floating point error being introduced](#). But, floating point error is introduced when two doubles of different magnitudes are subtracted, which is done here: 2388: d -= L\*ds; The check to exit the loop looks like this: 2410: if (!(d \*= 10.)) break; It compares the double value to zero. Unfortunately, there is floating point error introduced, and the value of "d" never gets down to zero. Therefore, the loop becomes infinite, and we keep appending characters to the output string, ignoring the specified size of the buffer. ( The buffer size test was done previously, based on the number of digits that it planned to place in the buffer ). My proposed fix is rather simple. Since we know up front how many digits we have to write out, we can use that number to specify the number of times that we loop, rather than depending on errorless floating point math. See the diff between the original and modified files attached. I changed the "for" line: From: for(i = 1; ; i++) { To: for(i = 1; i <= k+1; i++) { And, I removed the check on the bottom of the for loop. From: if (!(d \*= 10.)) break; To: d \*= 10.; Furthermore, the logic that is there is very bad. [Description about other problem cut, will file another bug where necessary.]

## Solution

They fixed [the calculations in the loop](#). [SIDE NOTE] Even though the bug looks like a simple error logic in a loop, from what I saw in the discussions, if they had used the Chrome's approach of isolating javascript objects, this bug would never be exploited. Why? In Chrome, Javascript objects are different (each plugin has its own JS objects), this means that plugins cannot interfere with each other nor the hosting application. Thus, even if a plug-in had decreased the floating precision, the crash would not occur. So the problem seems more like not properly isolating JS objects between plugins and Thunderbird

## Codes

"Overwrite memory"

---

## CVE-2005-0590

### Context

The underlying scenario is during an [installation](#), in which the application displays a [confirmation dialog](#) that shows a [spoofed URL](#).

### Problem

Between not checking for a [spoofed URL](#) with a username/password, and the unresizable, unwrapped [dialog for XPIInstall](#), it's possible to make a fairly convincing [spoofed URL for an XPI with InstallTrigger, due to incorrect parsing of the URL](#).

### Solution

The solution was to [strip user:pass from URL display](#). It added a function that does a preprocessing of the URL (nsXPITriggerItem::GetSafeURLString()).

### Codes

"Installer", "Spoofed origin of an install request", "Tricking user into installing a malicious plug-in"

---

## CVE-2004-0906

### Context

It happened at the [XPIInstall Engine](#)

### Problem

After installation, [many installed files are GROUP and WORLD writable](#), even though the installer was executed with the umask value 0022. In details: When [files are installed via XPIInstall, the user's umask is ignored](#). The XPIInstall engine [should respect the user's umask setting](#). The problem code is here: nsZipArchive::ExtractFile  
<http://lxr.mozilla.org/mozilla/source/modules/libjar/nsZipArchive.cpp#641> nsJAR::Extract  
<http://lxr.mozilla.org/mozilla/source/modules/libjar/nsJAR.cpp#251> both [open the file with 0644 perms and then chmod the file to the appropriate perms, but this sidesteps any umask](#). Just to make things more complicated, the nsZipArchive is part of standalone libjar, where PR\_Open is defined as fopen in zipstub.h, so passing the file's mode to PR\_Open wouldn't work in that situation.

In short, the extraction of extensions files was made [with wrong file permissions, creating world-readable/writeable files](#). This allows a [trojan to modify a benign application for malicious purposes](#).

### Solution

The fix was setting the [permissions on the extraction](#) function.

### Codes

"Installer", "Extracting the plug-in to world-accessible location", "Replace benign plugins by a malicious one"

---

## CVE-2004-0762

### Context

During [initialization of extensions](#)

### Problem

If a [malicious Web site can control or predict when and where a user will click](#), it can get [them to install software](#). Ways in which a Website can [predict user clicks](#):

1. A game. 1a. Make the player "pick up" items by clicking them. Measure the speed with which the player moves the mouse and clicks, and once the speed stabilizes, pop up an install dialog just before the player clicks. 1b. Force the player to click at exactly

the right time: a reaction-time test, shoot the monkey, etc. 1c. Convince the player to double-click an object whose location I control. 1d. Tell the player that he has infinite ammo and can shoot by pressing or holding the 'i' button on the keyboard. Pop up an install dialog when the player runs out of ammo.

2. Pop-up hell. 2a. Make the 'x' for the pop-up ad appear just where a security dialog will appear. 2b. Make fake pop-ups out of images so you can measure the victim's reaction time, average mouse acceleration, etc. Get them on the fifth "pop-up".

## Solution

They enumerated three possible alternatives, and decided to implement the following:

B) **Add a one-second delay between when the dialog gets focus and when the Install/OK button becomes enabled.** I say "gets focus" rather than "appears" because a site could hide an install dialog as a modal dialog of a background window for a minute and then bring the dialog to the front at a convenient time by closing the window in front.

The other alternatives were (but they're not implemented):

A) When a site tries to install software or calls enablePrivilege, display a status bar message, "This page would like to install software on your computer". Only display the dialog after the user clicks the status bar message. (Err, how do you click a status bar message with the keyboard?) C) If the total time to decide to install and download the xpi are less than five seconds, stall installation (with the "downloading..." dialog still up) until five seconds are up so the user has an extra chance to cancel. I'm worried that users might not know to cancel because they do not realize that they accidentally clicked "install" in a dangerous dialog.

## Codes

"Installer", "Not showing install warning dialog", "Silent install of plug-ins", "User-assisted attack"

# WordPress

---

## [CVE-2013-7279](#)

### Context

**Cross-site scripting (XSS)** vulnerability in views/video-management/preview\_video.php in the S3 Video plugin before 0.983 for WordPress allows remote attackers to **inject arbitrary web script or HTML via the base parameter**.

### Problem

S3 Video plugin for WordPress is vulnerable to **cross-site scripting**, caused by **improper validation of user-supplied input** by the preview\_video.php script. A remote attacker could exploit this vulnerability using the base parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to **steal the victim's cookie-based authentication credentials**.

### Solution

Fixed security issue and tested with Wordpress 3.8 **Fixed XSS scripting vulnerability** in video preview script

### Codes

"Arbitrary code execution", "Cross-site scripting (XSS)", "Steal credentials", "Unsanitized data", "Inject Javascript"

---

## [CVE-2013-5963](#)

### Context

WordPress allows remote attackers to **execute arbitrary code** by uploading a file with an executable extension, then accessing it via a direct request to the file in wp-content/uploads/wpdb/.

### Problem

#1.run the Firefox browser #2.Then **Add-ons Live HTTP headers in Firefox Install** >> #<https://addons.mozilla.org/en-us/firefox/addon/live-http-headers/> #3.Now the run Add-ons Live HTTP headers #4.Then go to this page site/[path]/wp-content/plugins/simple-dropbox-upload-form/multi.php?&height=500&width=1000&TB\_iframe=true #5.Click the Choose File button Then select a file [shell.jpg] #6.Then click on the Start upload button #7.Now using Live HTTP headers uploaded files to PHP change [shell.php] #8.Find your Shell site/wp-content/uploads/wpdb/shell.php

### Solution

**Removed multi.php**

### Codes

"File path traversal", "Lack of sandbox", "Unrestricted file upload"

---

## [CVE-2013-5098](#)

### Context

Download Monitor 'sort' Parameter **Cross Site Scripting Vulnerability**

### Problem

The Download Monitor plugin for WordPress is prone to a **cross-site scripting vulnerability** because it **fails to properly sanitize user-supplied input**. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to **steal cookie-based authentication credentials** and to launch other attacks.

### Solution

**Sanitized the sort parameter**, by invoking the function sanitize\_text\_field()

### Codes

"Cross-site scripting (XSS)", "Steal credentials", "Unsanitized data", "Sanitizing data"

---

## [CVE-2013-4954](#)

### Context

WordPress Pie Register Plugin 'wp-login.php' Multiple [Cross Site Scripting Vulnerabilities](#)

### Problem

Pie Register plugin for WordPress is prone to multiple [cross-site scripting vulnerabilities](#). An attacker may leverage these issues to [execute arbitrary script code](#) in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to [steal cookie-based authentication credentials](#) and launch other attacks. Input is not sanitized before being output on the screen:

```
<?php echo $_POST['pass1'];?>  
<?php echo $_POST['pass2'];?>
```

### Solution

[Escaping of HTML/Javascript](#) using `html_entity_decode`:

```
<?php echo htmlspecialchars($_POST['pass1']);?><?php echo htmlspecialchars($_POST['pass2']);?>
```

### Codes

"Arbitrary code execution", "Cross-site scripting (XSS)", "Steal credentials", "Escape user-supplied data"

---

## [CVE-2013-3532](#)

### Context

WordPress Spider Video Player Plugin 'theme' Parameter [SQL Injection Vulnerability](#)

### Problem

Spider Video Player plugin for WordPress is prone to an [SQL-injection vulnerability](#) because it [fails to sufficiently sanitize user-supplied data before using it in an SQL query](#). Exploiting this issue could allow an attacker to [compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database](#). Video Player Plugin for WordPress is [vulnerable to SQL injection](#). A remote attacker could send specially-crafted SQL statements to the settings.php script using the playlist and theme parameters, which could [allow the attacker to view, add, modify or delete information in the back-end database](#).

### Solution

[Sanitize input](#)

### Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2013-3529](#)

### Context

WordPress FuneralPress Plugin Multiple [HTML Injection Vulnerabilities](#)

### Problem

The FuneralPress plugin for WordPress is prone to multiple [HTML-injection vulnerabilities](#) because it [fails to properly sanitize user-supplied input](#). Attacker-supplied HTML and script code would [run in the context of the affected browser](#), potentially allowing the attacker to [control how the site is rendered](#) to the user. Other attacks are also possible.

### Solution

[sanitize text fields](#)

### Codes

## [CVE-2013-3526](#)

### Context

WordPress Traffic Analyzer Plugin 'aoid' [Parameter Cross Site Scripting Vulnerability](#).

### Problem

The Traffic Analyzer plugin for WordPress is prone to a cross-site scripting vulnerability because it [fails to properly sanitize user-supplied input](#). An attacker may leverage this issue to [execute arbitrary script code](#) in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to [steal cookie-based authentication credentials and launch other attacks](#).

### Solution

[sanitize input](#)

### Codes

"Cross-site scripting (XSS)", "Escape user-supplied data"

---

## [CVE-2013-3491](#)

### Context

WordPress Sharebar Plugin CVE-2013-3491 [Cross Site Request Forgery Vulnerability](#).

### Problem

The Sharebar plugin for WordPress is [prone to a cross-site request-forgery vulnerability](#). Exploiting this issue may allow a remote attacker to [perform certain unauthorized actions](#) in the context of the affected application. Other attacks are also possible.

### Solution

[sanitize input](#)

### Codes

"Privilege elevation", "Cross-site request forgery (CSRF)", "Lack of sandbox"

---

## [CVE-2013-3262](#)

### Context

Download Monitor 'p' Parameter [Cross Site Scripting Vulnerability](#).

### Problem

The Download Monitor plugin for WordPress is prone to a [cross-site scripting](#) vulnerability because it fails to [properly sanitize user-supplied input](#). An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to [steal cookie-based authentication credentials](#) and to launch other attacks.

### Solution

Description: **Note: This plugin is no longer actively developed nor maintained! However, a rewrite is planned.** -  
<http://mikejolley.com/2013/04/the-new-download-monitor-plugin/> Manage downloads on your site, view and show hits, and output in posts. sanitize\_text\_field to prevent XSS in admin

### Codes

"Cross-site scripting (XSS)", "Steal credentials", "Unsanitized data"

---

## [CVE-2013-3253](#)

## Context

WordPress Xhanch - My Twitter Plugin CVE-2013-3253 [Cross Site Request Forgery Vulnerability](#)

## Problem

The Xhanch - My Twitter plugin for WordPress is prone to a [cross-site request forgery vulnerability](#). Exploiting this issue may allow a remote attacker to [perform certain unauthorized actions](#) in the context of the affected application. Other attacks are also possible.

## Solution

[Security n hashtag](#)

## Codes

"Cross-site request forgery (CSRF)"

---

## [CVE-2013-2741](#)

## Context

The final step in the importbuddy backup restoration process is [supposed to remove importbuddy.php from the root of the site](#), however this [step often fails \(most commonly as a result of filesystem permissions\)](#) allowing an attacker [access to some or all of the functions and information provided](#) by importbuddy.php. An access password for importbuddy does not appear to be a mandatory requirement.

## Problem

The name of the backup file contains a random string [intended to prevent an attacker from guessing its value](#). However if backup files are present, browsing to <http://site/importbuddy.php> will expose their filenames; these [can then be used to download the files from the site](#): backup-zipfile-date-randomstring.zip. The desired backup file can be retrieved with: wget <http://site/backup-zipfile-date-randomstring.zip>. The backup consists of a zip archive containing the wordpress directory, complete with wp-config.php and often a .sql dump [containing a full copy of the wordpress database](#) and any other databases the backupbuddy plugin has been configured to include. Importbuddy also presents the option to upload a backup on step 1 of the restoration process, potentially allowing defacement or deletion and also trojanning the site if an existing backup is available. Additionally there are issues affecting the 'step' query string field. This has a [differing impact depending on the version of Backupbuddy targeted](#): <http://site/importbuddy.php?step=1>

## Solution

[Forcing the user to set a password](#) (and fixing the authentication bypass) would go some way to mitigating the risk of importbuddy.php not being deleted.

## Codes

"Overwrite files"

---

## [CVE-2013-2640](#)

## Context

WordPress [does not properly restrict access to unspecified Ajax functions](#), which allows remote attackers to [modify plugin settings and conduct cross-site scripting \(XSS\) attacks](#) via unspecified vectors related to "formData=save" requests

## Problem

WordPress [does not properly restrict access to unspecified Ajax functions](#), which allows remote attackers to [modify plugin settings and conduct cross-site scripting \(XSS\) attacks](#) via unspecified vectors related to "formData=save" requests

## Solution

Security vulnerability has been [patched with is\\_user\\_logged\\_in\(\)](#) and now submitted to first review

## Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Not enforcing private code"

---

## [CVE-2013-2501](#)

### Context

WordPress Terillion Reviews Plugin Profile Id [HTML Injection Vulnerability](#)

### Problem

The Terillion Reviews plugin for WordPress is prone to an [HTML-injection vulnerability](#) because it [fails to properly sanitize user-supplied input before using it in dynamically generated content](#). Successful exploits will allow [attacker-supplied HTML and script code to run](#) in the context of the affected browser, potentially allowing the attacker to [steal cookie-based authentication credentials](#) or to [control how the site is rendered to the user](#). Other attacks are also possible.

### Solution

Fix security vulnerability by [sanitizing user input](#)

### Codes

"Cross-site scripting (XSS)", "Lack of sandbox"

---

## [CVE-2013-2204](#)

### Context

[Content Spoofing](#) in the MoxieCode (TinyMCE) MoxiePlayer project

### Problem

[Flash doesn't recognize '#' symbol as the beginning of the fragment to ignore](#), so if '?' mark follows, remaining part of the url will still be [interpreted as application parameters...](#)

### Solution

[Consider part of url after '?' as querystring](#), no matter what precedes it.

### Codes

"Lack of sandbox", "Content spoofing"

---

## [CVE-2013-1464](#)

### Context

WordPress Audio Player SWF [Cross Site Scripting](#)

### Problem

WordPress Audio Player Plugin 'playerID' Parameter [Cross Site Scripting Vulnerability](#) The Audio Player plugin for WordPress is prone to a cross-site scripting vulnerability because it [fails to properly sanitize user-supplied input](#). An attacker may leverage this issue to [execute arbitrary script code](#) in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to [steal cookie-based authentication credentials and launch other attacks](#).

### Solution

[sanitize input](#)

### Codes

"Cross-site scripting (XSS)", "HTML Injection", "Inject Javascript"

---

## [CVE-2013-1409](#)

### Context

[Cross-Site Scripting \(XSS\)](#) in CommentLuv wordpress plugin

## Problem

The vulnerability exists due to **insufficient filtration of user-supplied data** in "\_ajax\_nonce" HTTP POST parameter in the "/wp-admin/admin-ajax.php" script. A remote attacker can trick a logged-in administrator to open a specially crafted link and **execute arbitrary HTML and script code in browser** in context of the vulnerable website. PoC (Proof-of-Concept) below uses the "alert()" JavaScript function to display administrator's cookies

## Solution

Upgrade to CommentLuv 2.92.4

**filter user supplied data**

## Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Lack of sandbox"

---

## [CVE-2013-0735](#)

### Context

WordPress Mingle Forum Plugin Multiple **SQL Injection and Cross Site Scripting Vulnerabilities**

## Problem

The Mingle Forum plug-in for WordPress is prone to **multiple SQL-injection and cross-site scripting vulnerabilities** because it **fails to sufficiently sanitize user-supplied input**. Exploiting these vulnerabilities could allow an attacker to **steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database**.

## Solution

**sanitize user-supplied data**

## Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2013-0734](#)

### Context

WordPress Mingle Forum Plugin Multiple **SQL Injection and Cross Site Scripting Vulnerabilities**

## Problem

The Mingle Forum plug-in for WordPress is prone to **multiple SQL-injection and cross-site scripting vulnerabilities** because it **fails to sufficiently sanitize user-supplied input**. Exploiting these vulnerabilities could allow an attacker to **steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database**.

## Solution

**sanitize user-supplied data**

## Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2013-0731](#)

### Context

WordPress MailUp Plugin **Security Bypass Vulnerability**

## Problem

WordPress **does not properly restrict access** to unspecified Ajax functions, which **allows remote attackers to modify plugin settings and conduct cross-site scripting (XSS)** attacks by setting the wordpress\_logged\_in cookie.

## Solution

Security vulnerability has been [patched with is\\_user\\_logged\\_in\(\)](#) and now submitted to first review

## Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Not enforcing private code", "Bypass protection mechanism"

---

## CVE-2012-6527

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in the My Calendar plugin before 1.10.2 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the PATH\_INFO.

### Problem

My Calendar plugin for WordPress is [vulnerable to cross-site scripting](#), caused by [improper validation of user-supplied input](#). A remote attacker could exploit this vulnerability using a specially-crafted URL to [execute script in a victim's Web browser within the security context of the hosting Web site](#), once the URL is clicked. An attacker could use this vulnerability to [steal the victim's cookie-based authentication credentials](#).

### Solution

[escape urls before use](#). Confirm that event ids are integers.

## Codes

"Cross-site scripting (XSS)", "Inject Javascript", "Sanitize data (enforce expected datatype)", "User-assisted attack"

---

## CVE-2012-5328

### Context

[Multiple SQL injection vulnerabilities](#) in the Mingle Forum plugin 1.0.32.1 and other versions before 1.0.33 for WordPress might allow remote authenticated users to [execute arbitrary SQL commands](#) via the (1) memberid or (2) groupid parameters in a removemember action or (3) id parameter to fs-admin/fs-admin.php, or (4) edit\_forum\_id parameter in an edit\_save\_forum action to fs-admin/wpf-edit-forum-group.php.

### Problem

[Sql injection vulnerabilities.](#)

### Solution

[escape data in post request](#) before performing sql operations.

## Codes

"SQL injection", "Unrestricted access to database"

---

## CVE-2012-5327

### Context

[Multiple SQL injection vulnerabilities](#) in fs-admin/fs-admin.php in the Mingle Forum plugin 1.0.32.1 and other versions before 1.0.33 for WordPress allow remote authenticated users to [execute arbitrary SQL commands](#) via the (1) delete\_usrgrp[] parameter in a delete\_usergroups action, (2) usergroup parameter in an add\_user\_togroup action, or (3) add\_forum\_group\_id parameter in an add\_forum\_submit action.

### Problem

WordPress Mingle Forum Plugin is [vulnerable to SQL injection](#). A remote attacker could send specially-crafted SQL statements to the admin.php script using the multiple parameters, which could allow the attacker to [view, add, modify or delete information in the back-end database](#).

## Solution

[escape data in post requests](#) before doing database operations.

## Codes

"Escape user-supplied data", "SQL injection"

---

## CVE-2012-4283

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in the Login With Ajax plugin before 3.0.4.1 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the callback parameter.

### Problem

[XSS](#) in Login with Ajax plugin

### Solution

[use regex to match the expected query string](#)

### Codes

"Cross-site scripting (XSS)", "Unsanitized data", "HTML Injection", "Inject Javascript"

---

## CVE-2012-4273

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in libs/xing.php in the 2 Click Social Media Buttons plugin before 0.34 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the xing-url parameter.

### Problem

2 Click Social Media Buttons plugin for WordPress is vulnerable to [cross-site scripting](#), caused by [improper validation of user-supplied input](#) by the xing.php script. A remote attacker could exploit this vulnerability using the xing-url parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to [steal the victim's cookie-based authentication credentials](#).

### Solution

[strip tags from url](#)

### Codes

"Perform security check on unsanitized data", "Cross-site scripting (XSS)"

---

## CVE-2012-4272

### Context

[Multiple cross-site scripting \(XSS\) vulnerabilities](#) in the 2 Click Social Media Buttons plugin before 0.34 for WordPress allow remote attackers to [inject arbitrary web script or HTML](#) via unspecified vectors related to the "processing of the buttons of Xing and Pinterest".

### Problem

[XSS vulnerabilities](#) in Click Social Media Buttons plugin

### Solution

[strip tags before decoding raw url](#)

### Codes

"Perform security check on unsanitized data", "Cross-site scripting (XSS)", "Unsanitized data"

---

## [CVE-2012-4271](#)

### Context

[Multiple cross-site scripting \(XSS\) vulnerabilities](#) in bad-behavior-wordpress-admin.php in the Bad Behavior plugin before 2.0.47 and 2.2.x before 2.2.5 for WordPress allow remote attackers to [inject arbitrary web script or HTML](#) via the (1) PATH\_INFO, (2) httpbl\_key, (3) httpbl\_maxage, (4) httpbl\_threat, (5) reverse\_proxy\_addresses, or (6) reverse\_proxy\_header parameter.

### Problem

Bad Behavior plugin for WordPress is vulnerable to [cross-site scripting](#), caused by [improper validation of user-supplied input](#) by the options-general.php script. A remote attacker could exploit this vulnerability using multiple parameters in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to [steal the victim's cookie-based authentication credentials](#).

### Solution

[escape url before use \(sanitize\)](#)

### Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Escape user-supplied data"

---

## [CVE-2012-4268](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in bulletproof-security/admin/options.php in the BulletProof Security plugin before .47.1 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the HTTP\_ACCEPT\_ENCODING header.

### Problem

BulletProof Security plugin for WordPress is vulnerable to [cross-site scripting, caused by improper validation of user-supplied input](#) by the admin.php script. A remote attacker could exploit this vulnerability using the page parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker [could use this vulnerability to steal the victim's cookie-based authentication credentials](#).

### Solution

[filter and sanitize input string](#) before use.

### Codes

"Steal data", "Cross-site scripting (XSS)"

---

## [CVE-2012-4264](#)

### Context

[Multiple cross-site scripting \(XSS\) vulnerabilities](#) in the Better WP Security (better\_wp\_security) plugin before 3.2.5 for WordPress allow remote attackers to [inject arbitrary web script or HTML](#) via unspecified vectors related to "server variables," a different vulnerability than CVE-2012-4263.

### Problem

[XSS vulnerabilities](#) in Better WP Security plugin

### Solution

[filter and sanitize string](#) before use.

### Codes

"Arbitrary code execution", "Cross-site scripting (XSS)", "Unsanitized data"

---

## [CVE-2012-4263](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in inc/admin/content.php in the Better WP Security (better\_wp\_security) plugin before 3.2.5 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the HTTP\_USER\_AGENT header.

### Problem

The value of the User-Agent HTTP header is [copied into the HTML document as plain text between tags](#). The payload a712378089b4648b was submitted in the User-Agent HTTP header. This input was echoed unmodified in the application's response. This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. Issue background [Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way](#). An attacker can use the vulnerability to construct a request which, if issued by another application user, will cause JavaScript code supplied by the attacker to [execute within the user's browser in the context of that user's session with the application](#). The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes. Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site which causes anyone viewing it to [make arbitrary cross-domain requests to the vulnerable application](#) (using either the GET or the POST method). The security impact of cross-site scripting vulnerabilities is [dependent upon the nature of the vulnerable application](#), the kinds of data and functionality which it contains, and the other applications which belong to the same domain and organisation. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain which can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organisation which owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by [injecting Trojan functionality into the vulnerable application, and exploiting users' trust in the organisation in order to capture credentials for other applications which it owns](#). In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk. Issue remediation In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defences: Input should be validated as strictly as possible on arrival, given the kind of content which it is expected to contain.

For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitised. User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including <> " and =, should be replaced with the corresponding HTML entities (<> etc). In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

*Exploit Example:*

#### Request

```
GET /wp-admin/admin.php?page=better_wp_security HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0)
Gecko/20100101 Firefox/11.0a7123<script>alert(1)</script>78089b4648b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Referer: http://127.0.0.1/wp-admin/options-general.php
Cookie:
wordpress_5c016e8f0f95f039102cbe8366c5c7f3=admin%7C1333587813%7C73fe3e4d525d2460588947c4b7a03114;
wp-settings-1=widgets_access%3Doff%26uploader%3D1;
wp-settings-time-1=1333368822; wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_5c016e8f0f95f039102cbe8366c5c7f3=admin%7C1333587813%7C7b961d6e5caea2c784f282c5ed426964;
bb2_screener_=1333415711+127.0.0.1; PHPSESSID=j3l493obmauq7akebg8g3jb4k3
```

#### Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 03 Apr 2012 02:05:00 GMT
Server: Apache/2.2.20 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.6
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Last-Modified: Tue, 03 Apr 2012 02:05:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 35849
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<!--[if IE 8]>
<html xmlns="http://www.w3.org/1999/xhtml" class="ie8" dir="ltr" lang="en-US">
<![endif]-->
<!--[if !(IE 8) ]><!-->
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr"
...[SNIP]...
<strong>Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0)
Gecko/20100101
Firefox/11.0a7123<script>alert(1)</script>|Injected Script|78089b4648b</strong>
```

## Solution

[Better Sanitization](#) to eliminate possible XSS attacks

## Codes

"Arbitrary code execution", "Cross-site scripting (XSS)", "Sanitize data (enforce expected datatype)"

---

## [CVE-2012-3576](#)

### Context

[Unrestricted file upload vulnerability](#) in php/upload.php in the wpStoreCart plugin before 2.5.30 for WordPress allows remote attackers to [execute arbitrary code by uploading a file with an executable extension](#), then accessing it via a direct request to the file in uploads/wpstystorecart.

### Problem

wpStoreCart plugin for WordPress could allow a remote attacker to [upload arbitrary files, caused by the improper validation of file extensions](#) by the upload.php script. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to [upload a malicious PHP script, which could allow the attacker to execute arbitrary PHP code on the vulnerable system](#).

## Solution

[validate file extensions](#)

## Codes

"Lack of sandbox", "Unrestricted file upload"

---

## [CVE-2012-2920](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in the userphoto\_options\_page function in user-photo.php in the User Photo plugin before 0.9.5.2 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the PATH\_INFO to wp-admin/options-general.php. NOTE: some of these details are obtained from third party information.

### Problem

User Photo plugin for WordPress is vulnerable to [cross-site scripting](#), caused by improper validation of user-supplied input by the options-general.php script. A remote attacker could exploit this vulnerability using the '\$\_SERVER['REQUEST\_URI']' parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to [steal the victim's cookie-based authentication credentials](#).

#### Solution

[escape url before use](#)

#### Codes

"Unsanitized parameter", "Cross-site scripting (XSS)", "Escape user-supplied data"

---

## [CVE-2012-2916](#)

#### Context

[Cross-site scripting \(XSS\) vulnerability](#) in sabre\_class\_admin.php in the SABRE plugin before 2.1 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the active\_option parameter to wp-admin/tools.php.

#### Problem

SABRE plugin for WordPress is [vulnerable to cross-site scripting](#), caused by [improper validation of user-supplied input](#) by the tools.php script. A remote attacker could exploit this vulnerability using the active\_option parameter in a specially-crafted URL to [execute script in a victim's Web browser within the security context of the hosting Web site](#), once the URL is clicked. An attacker could use this vulnerability to [steal the victim's cookie-based authentication credentials](#).

#### Solution

[sanitize text before using it.](#)

#### Codes

"Unsanitized parameter", "Cross-site scripting (XSS)", "Inject Javascript", "Not escaping characters"

---

## [CVE-2012-2759](#)

#### Context

[Cross-site scripting \(XSS\) vulnerability](#) in login-with-ajax.php in the Login With Ajax (aka login-with-ajax) plugin before 3.0.4.1 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the callback parameter in a lostpassword action to wp-login.php.

#### Problem

Login With Ajax plugin for WordPress is vulnerable to [cross-site scripting](#), caused by improper validation of user-supplied input by the login-with-ajax.php script. A remote attacker could exploit this vulnerability using the [JSON callback parameter](#) in a specially-crafted URL to [execute script in a victim's Web browser](#) within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to [steal the victim's cookie-based authentication credentials](#).

#### Solution

[Sanitize data before use](#)

#### Codes

"Unsanitized parameter", "Cross-site scripting (XSS)", "Sanitize data (enforce expected datatype)"

---

## [CVE-2012-2402](#)

#### Context

wp-admin/plugins.php in WordPress before 3.3.2 allows remote authenticated site administrators to [bypass intended access restrictions and deactivate network-wide plugins](#) via unspecified vectors.

## Problem

WordPress could allow a remote attacker to [bypass security restrictions](#), caused by an error in plugins.php when handling network wide plugins. A remote attacker could exploit this vulnerability to [bypass security restrictions and gain unauthorized administrative access to the vulnerable application](#).

## Solution

[check that the authenticated user is a wp admin](#) before allowing them to disable plugins

## Codes

---

## [CVE-2012-1785](#)

### Context

kg\_callffmpeg.php in the Video Embed & Thumbnail Generator plugin before 2.0 for WordPress allows remote attackers to [execute arbitrary commands](#) via unspecified vectors.

## Problem

Video Embed & Thumbnail Generator plugin for WordPress could allow a remote attacker to execute arbitrary code on the system, caused by the [improper validation of user-supplied input](#) in exec() function by the kg\_callffmpeg.php script. By persuading a victim to visit a specially-crafted Web page, a remote attacker could exploit this vulnerability to [inject and execute arbitrary shell code](#) on the vulnerable system.

## Solution

[validate input before using](#)

## Codes

"Steal data", "Cross-site scripting (XSS)", "improper validation of user-supplied input"

---

## [CVE-2012-1205](#)

### Context

PHP [remote file inclusion vulnerability](#) in relocate-upload.php in Relocate Upload plugin before 0.20 for WordPress allows remote attackers to [execute arbitrary PHP code](#) via a URL in the abspath parameter.

## Problem

[Allowed anybody in include remote files](#)

## Solution

Adopted proper 'wp\_ajax\_' action, to close off a major security issue. [only admin should have access to certain actions](#) ('wp\_ajax\_relocate\_upload', 'relocate\_upload\_js\_action')

## Codes

---

## [CVE-2012-1125](#)

### Context

[Unrestricted file upload vulnerability](#) in uploadify/scripts/uploadify.php in the Kish Guest Posting plugin before 1.2 for WordPress allows remote attackers to [execute arbitrary code by uploading a file with a PHP extension](#), then accessing it via a direct request to the file in the directory specified by the folder parameter.

## Problem

Kish Guest Posting plugin for WordPress could allow a remote attacker to upload arbitrary files, caused by the [improper validation of file extensions](#) by the uploadify.php script. By sending a direct request using the folder parameter, a remote attacker could exploit this vulnerability to [upload a malicious PHP script](#), which could allow the attacker to execute arbitrary PHP code on the vulnerable system.

## Solution

[Check the extension of the file](#) to make sure its an allowable type. [Do not allow folder creation.](#)

## Codes

"Unsanitized data", "Lack of sandbox", "Unrestricted file upload"

---

## CVE-2012-1068

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in the rc\_ajax function in core.php in the WP-RecentComments plugin before 2.0.7 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the page parameter, related to AJAX paging.

### Problem

WP-RecentComments Plugin for WordPress is vulnerable to [cross-site scripting](#), caused by [improper validation of user-supplied input](#) by the core.php script. A remote attacker could exploit this vulnerability using the page parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to [steal the victim's cookie-based authentication credentials](#).

## Solution

[sanitize input](#) (make sure page is an int) before using the data.

## Codes

"Cross-site scripting (XSS)", "Unsanitized data", "improper validation of user-supplied input", "Sanitize data (enforce expected datatype)"

---

## CVE-2012-1011

### Context

actions.php in the AllWebMenus plugin 1.1.8 for WordPress allows remote attackers to [bypass intended access restrictions to upload and execute arbitrary PHP code](#) by setting the HTTP\_REFERER to a certain value, then uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.

### Problem

WordPress AllWebMenus Plugin could allow a remote attacker to upload arbitrary files, [caused by the improper validation of file extensions](#) by the actions.php script. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious PHP script, which could allow the attacker to [execute arbitrary PHP code on the vulnerable system](#). lack of checks in script actions.php allowed malicious user to upload any file to the vulnerable server. Create a file (For example, Wordpress\_security.php, with this content: echo <php echo '6Scan to the rescue'; ?>. Compress it with zip to awm.zip

## Solution

[checks the source referrer](#)

## Codes

"Unrestricted file upload"

---

## CVE-2012-1010

### Context

[Unrestricted file upload vulnerability](#) in actions.php in the AllWebMenus plugin before 1.1.8 for WordPress allows remote attackers to [execute arbitrary PHP code](#) by uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.

### Problem

WordPress AllWebMenus Plugin could allow a remote attacker to upload arbitrary files, [caused by the improper validation of file extensions](#) by the actions.php script. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to

[upload a malicious PHP script](#), which could allow the attacker to execute arbitrary PHP code on the vulnerable system. lack of checks in script actions.php allowed [malicious user to upload any file to the vulnerable server](#).

## Solution

[checks the source referrer](#),

## Codes

"Lack of sandbox", "Unrestricted file upload"

---

## CVE-2012-0934

### Context

[PHP remote file inclusion vulnerability](#) in ajax/savetag.php in the Theme Tuner plugin for WordPress before 0.8 allows remote attackers to [execute arbitrary PHP code](#) via a URL in the tt-abspath parameter.

### Problem

WordPress Theme Tuner Plugin could [allow a remote attacker to include arbitrary files](#). A remote attacker could send a specially-crafted URL request to the savetag.php script using the tt-abspath parameter to specify a malicious file from a remote system, which could allow the attacker to [execute arbitrary code on the vulnerable Web server](#).

## Solution

[sanitize data before using it](#)

## Codes

"Remote Code Execution", "File path traversal", "Remote file inclusion"

---

## CVE-2011-5264

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in lazyest-backup.php in the Lazyest Backup plugin before 0.2.2 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the xml\_or\_all parameter

### Problem

Lazyest Backup Plugin for WordPress is vulnerable to [cross-site scripting](#), caused by [improper validation of user-supplied input](#). A remote attacker could exploit this vulnerability using the [xml\\_or\\_all](#) parameter in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

## Solution

[sanitize input](#) before using it

## Codes

"Steal data", "Perform security check on unsanitized data", "Unsanitized parameter", "Cross-site scripting (XSS)"

---

## CVE-2011-5226

### Context

[Cross-site request forgery \(CSRF\) vulnerability](#) in wordpress\_sentinel.php in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to [hijack the authentication of an administrator](#) for requests that trigger snapshots.

### Problem

Sentinel Plugin for WordPress is vulnerable to [cross-site request forgery](#), caused by [improper validation of user-supplied input](#). By [persuading an authenticated user to visit a malicious Web site](#), a remote attacker could send a malformed HTTP request to perform

**Unauthorized actions.** An attacker could exploit this vulnerability to perform cross-site scripting attacks, Web cache poisoning, and other malicious activities.

## Solution

escape html before using the input (sanitize)

## Codes

"Unsanitized data", "Cross-site request forgery (CSRF)", "Lack of sandbox"

---

## CVE-2011-5225

### Context

Cross-site scripting (XSS) vulnerability in wordpress\_sentinel.php in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via unknown vectors.

### Problem

Sentinel Plugin for WordPress is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

## Solution

sanitize input before use

## Codes

"Perform security check on unsanitized data", "Unsanitized parameter", "Cross-site scripting (XSS)"

---

## CVE-2011-5224

### Context

SQL injection vulnerability in the Sentinel plugin 1.0.0 for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors.

### Problem

Sentinel Plugin for WordPress is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements which could allow the attacker to view, add, modify or delete information in the back-end database.

## Solution

validate data before using it for sql operations

## Codes

"SQL injection", "Unrestricted access to database"

---

## CVE-2011-5216

### Context

SQL injection vulnerability in ajax.php in SCORM Cloud For WordPress plugin before 1.0.7 for WordPress allows remote attackers to execute arbitrary SQL commands via the active parameter

### Problem

SCORM Cloud for WordPress is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements to the ajax.php script using the active parameter, which could allow the attacker to view, add, modify or delete information in the back-end database.

## Solution

**validate data** before performing sql operations

## Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2011-5194](#)

### Context

**Cross-site scripting (XSS) vulnerability** in vendors/samswhois/samswhois.inc.php in the Whois Search plugin before 1.4.2.3 for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the domain parameter, a different vulnerability than CVE-2011-5193.

### Problem

The domain parameter allows for **XSS**

### Solution

**Validate input around the domain parameter**

### Codes

"Cross-site scripting (XSS)", "Unsanitized data"

---

## [CVE-2011-5192](#)

### Context

**Cross-site scripting (XSS) vulnerability** in pretty-bar.php in Pretty Link Lite plugin before 1.5.6 for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the slug parameter, a different vulnerability than CVE-2011-5191.

### Problem

**Characters are not escaped around the slug parameter** and allows for XSS.

### Solution

Fixed a **cross-site scripting vulnerability**, that could have affected a very small number of users Fix XSS near the slug parameter

### Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Escape user-supplied data"

---

## [CVE-2011-5191](#)

### Context

**Cross-site scripting (XSS) vulnerability** in pretty-bar.php in Pretty Link Lite plugin before 1.5.4 for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the slug parameter, a different vulnerability than CVE-2011-5192.

### Problem

Pretty link lite plugin allows **XSS through** via the slug parameter

### Solution

Fixed an issue with Pretty Link Export link for Pro users **check input to make sure XSS is not possible**

### Codes

"Perform security check on unsanitized data", "Cross-site scripting (XSS)", "Unsanitized data"

---

## [CVE-2011-5181](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in clickdesk.php in ClickDesk Live Support - Live Chat plugin 2.0 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the cdwidgetid parameter. NOTE: some of these details are obtained from third party information.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/36338/> ClickDesk Live Support plugin for WordPress is prone to a [cross-site-scripting vulnerability because it fails to properly sanitize user-supplied input](#). An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. [This can allow the attacker to steal cookie-based authentication credentials and launch other attacks](#). [http://www.example.com/\[path\]/wp-content/plugins/clickdesk-live-support-chat/clickdesk.php?cdwidgetid=\[xss\]](http://www.example.com/[path]/wp-content/plugins/clickdesk-live-support-chat/clickdesk.php?cdwidgetid=[xss])

### Solution

Not found

### Codes

"Cross-site scripting (XSS)", "Unsanitized data"

---

## [CVE-2011-5180](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in wp-1pluginjquery.php in the ZooEffect plugin 1.01 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the page parameter. NOTE: some of these details are obtained from third party information. NOTE: this has been disputed by a third party.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/36323/>

1-jquery-photo-gallery-slideshow-flash plug-in for WordPress is prone to a [cross-site-scripting vulnerability](#) because it [fails to sufficiently sanitize user-supplied data](#). An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. [http://www.example.com/\[path\]/wp-content/plugins/1-jquery-photo-gallery-slideshow-flash/wp-1pluginjquery.php?page=\[xss\]](http://www.example.com/[path]/wp-content/plugins/1-jquery-photo-gallery-slideshow-flash/wp-1pluginjquery.php?page=[xss])

### Solution

Not found

### Codes

"Cross-site scripting (XSS)", "Unsanitized data"

---

## [CVE-2011-5128](#)

### Context

[Multiple cross-site scripting \(XSS\) vulnerabilities](#) in the Adminimize plugin before 1.7.22 for WordPress allow remote attackers to [inject arbitrary web script or HTML](#) via the page parameter to (1) inc-options/deinstall\_options.php, (2) inc-options/theme\_options.php, or (3) inc-options/im\_export\_options.php, or the (4) post or (5) post\_ID parameters to adminimize.php, different vectors than CVE-2011-4926.

### Problem

Adminimize plugin does [not escape html attributes](#) in several parameters which enables users to perform [XSS](#)

### Solution

## Escape html attributes in user input

### Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Not escaping characters"

---

## CVE-2011-5107

### Context

**Cross-site scripting (XSS) vulnerability** in post\_alert.php in Alert Before Your Post plugin, possibly 0.1.1 and earlier, for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the name parameter.

### Problem

(Based on exploit)

"Alert Before Your Post" plugin for WordPress is prone to a **cross-site scripting** vulnerability because it fails to **properly sanitize user-supplied input**. An attacker may leverage this issue to **execute arbitrary script code** in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal **cookie-based authentication credentials** and launch other attacks.  
[http://www.example.com/\[path\]/wp-content/plugins/alert-before-your-post/trunk/post\\_alert.php?name=\[xss\]](http://www.example.com/[path]/wp-content/plugins/alert-before-your-post/trunk/post_alert.php?name=[xss])

### Solution

**Properly Sanitize Input**

### Codes

"Arbitrary code execution", "Steal data", "Unsanitized parameter", "Cross-site scripting (XSS)", "Steal credentials", "Unsanitized data"

---

## CVE-2011-5106

### Context

**Cross-site scripting (XSS) vulnerability** in edit-post.php in the Flexible Custom Post Type plugin before 0.1.7 for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the id parameter.

### Problem

When querying the id of the post, the Flexible Custom Type Plugin **doesn't make sure the id is an integer**, which allows users to perform **XSS**

### Solution

**Make sure the id of the post is an integer**

### Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Sanitize data (enforce expected datatype)"

---

## CVE-2011-5104

### Context

**Cross-site scripting (XSS) vulnerability** in wpsc-admin/display-sales-logs.php in WP e-Commerce plugin 3.8.7.1 and possibly earlier for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the custom\_text parameter.

### Problem

The custom-text parameter input is **not escaped** for html attributes which causes the potential for **XSS**

### Solution

**Escape** the html attributes in custom-text parameter

### Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Not escaping characters"

---

## [CVE-2011-4926](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in adminimize/adminimize\_page.php in the Adminimize plugin before 1.7.22 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the page parameter.

### Problem

The user input in page parameter is [not escaped](#) which causes the potential for [XSS](#)

### Solution

[Escape user input](#) in page parameter

### Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Not escaping characters"

---

## [CVE-2011-4803](#)

### Context

[SQL injection vulnerability](#) in wptouch/ajax.php in the WPtouch plugin for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the id parameter.

### Problem

The [id variable is not checked](#) if it's an id number, which causes the potential to [execute arbitrary SQL commands](#).

### Solution

[Sanitize user input](#)

### Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2011-4673](#)

### Context

[SQL injection vulnerability](#) in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the id parameter.

### Problem

Based on exploit The [id parameter is not checked](#) if it's a valid id number, which causes the potential to [execute arbitrary SQL commands](#)

### Solution

[Sanitize User input](#)

### Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2011-4671](#)

## Context

[SQL injection vulnerability](#) in adrotate/adrotate-out.php in the AdRotate plugin 3.6.6, and other versions before 3.6.8, for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the track parameter (aka redirect URL).

## Problem

Based on exploit \$wpdb->prepare can be misused to include a query, since [no check is implemented on it.](#)

## Solution

Not found

## Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2011-4646](#)

### Context

[SQL injection vulnerability](#) in wp-postratings.php in the WP-PostRatings plugin 1.50, 1.61, and probably other versions before 1.62 for WordPress allows remote authenticated users with the Author role to [execute arbitrary SQL commands](#) via the id attribute of the ratings shortcode when creating a post. NOTE: some of these details are obtained from third party information.

## Problem

In the rating attribute, the input provided by the user was [not escaped which caused the potential for code injection](#)

## Solution

[Escape the html attributes](#) in the rating attribute

## Codes

"Cross-site scripting (XSS)", "Not escaping characters", "Code Injection"

---

## [CVE-2011-4618](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in advancedtext.php in Advanced Text Widget plugin before 2.0.2 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the page parameter.

## Problem

Characters received by the user for page parameter are [not being escaped which causes the potential for XSS](#)

## Solution

[Escape characters from user input](#)

## Codes

"Cross-site scripting (XSS)", "Unsanitized data", "HTML Injection", "Inject Javascript", "Not escaping characters", "Code Injection"

---

## [CVE-2011-4568](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in view/frontend-head.php in the Flowplayer plugin before 1.2.12 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the URI.

## Problem

[VAGUE] the Requested URI from the Server was **not being encoded**, which created the option for users to **XSS** through this parameter.

## Solution

**Encode the requested URI**

## Codes

"Unsanitized parameter", "Cross-site scripting (XSS)", "Unsanitized data"

---

## CVE-2011-4562

### Context

**Multiple cross-site scripting (XSS) vulnerabilities** in (1) view/admin/log\_item.php and (2) view/admin/log\_item\_details.php in the Redirection plugin 2.2.9 for WordPress allow remote attackers to **inject arbitrary web script or HTML** via the Referer HTTP header in a request to a post that does not exist.

### Problem

In multiple files, characters provided by the user are **not escaped which causes the potential for XSS**

## Solution

**Escape characters** from user input to disable XSS

## Codes

"Cross-site scripting (XSS)", "Unsanitized data", "Escape user-supplied data", "Not escaping characters"

---

## CVE-2011-4342

### Context

**PHP remote file inclusion vulnerability** in wp\_xml\_export.php in the BackWPup plugin before 1.7.2 for WordPress allows remote attackers to **execute arbitrary PHP code** via a URL in the wpabs parameter.

### Problem

A vulnerability has been discovered in the Wordpress plugin BackWPup 1.6.1 which can be exploited to **execute local or remote code on the web server**. The Input passed to the component "wp\_xml\_export.php" via the "wpabs" variable allows the inclusion and execution of local or remote PHP files as long as a "\_nonce" value is known. The "\_nonce" value relies on a static constant which is not defined in the script meaning that it defaults to the value "822728c8d9".

## Solution

Not found

## Codes

"Remote Code Execution", "Lack of sandbox", "inject code"

---

## CVE-2011-3981

### Context

**PHP remote file inclusion vulnerability** in actions.php in the Allwebmenus plugin 1.1.3 for WordPress allows remote attackers to **execute arbitrary PHP code** via a URL in the abspath parameter.

### Problem

Attackers can execute PHP in header paths since there is **no check if the file being attached exists locally**, and there is **no escaping of characters**.

## Solution

Add a check to see if the file exists locally and escape certain characters.

## Codes

"Remote Code Execution", "Lack of sandbox"

---

## CVE-2011-1047

### Context

Multiple SQL injection vulnerabilities in VastHTML Forum Server (aka ForumPress) plugin 1.6.1 and 1.6.5 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) search\_max parameter in a search action to index.php, which is not properly handled by wpf.class.php, (2) id parameter in an editpost action to index.php, which is not properly handled by wpf-post.php, or (3) topic parameter to feed.php.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/16235/> The vulnerability exists due to failure in the "index.php" script to properly sanitize user-supplied input in "search\_max" variable. Attacker can alter queries to the application SQL database, execute arbitrary queries to the database, compromise the application, access or modify sensitive data, or exploit various vulnerabilities in the underlying SQL database.

## Solution

Sanitize user input

## Codes

"SQL injection", "Unrestricted access to database"

---

## CVE-2010-5295

### Context

Cross-site scripting (XSS) vulnerability in wp-admin/plugins.php in WordPress before 3.0.2 might allow remote attackers to inject arbitrary web script or HTML via a plugin's author field, which is not properly handled during a Delete Plugin action.

### Problem

The name and author field of a plugin could inject code which would be executed when trying to delete a plugin.

## Solution

Escape correctly the strings of name and author fields when trying to delete a plugin, so that they're safe to be used in HTML.

## Codes

"Cross-site scripting (XSS)", "HTML Injection", "Inject Javascript", "Not escaping characters", "Code Injection"

---

## CVE-2010-4839

### Context

SQL injection vulnerability in the Event Registration plugin 5.32 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the event\_id parameter in a register action.

### Problem

Based on exploit The event\_id parameter is not checked properly, which enables users to inject SQL commands through it.

## Solution

**Based on exploit: sanitize user input**

#### Codes

"SQL injection", "Unrestricted access to database"

---

### CVE-2010-4747

#### Context

**Cross-site scripting (XSS) vulnerability** in wordpress-processing-embed/data/popup.php in the Processing Embed plugin 0.5 for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the pluginurl parameter.

#### Problem

Based on exploit: <https://www.exploit-db.com/exploits/35066/> The Processing Embed plugin for Wordpress is prone to a **cross-site-scripting vulnerability because it fails to properly sanitize user-supplied input** in pluginurl parameter. An attacker may leverage this issue to **execute arbitrary script code in the browser** of an unsuspecting user in the context of the affected site. This can allow the attacker to **steal cookie-based authentication credentials and launch other attacks**.

#### Solution

Based on exploit: **sanitize user input**

#### Codes

"Cross-site scripting (XSS)", "HTML Injection", "Inject Javascript", "Code Injection"

---

### CVE-2010-4518

#### Context

**Cross-site scripting (XSS) vulnerability** in wp-safe-search/wp-safe-search-jx.php in the Safe Search plugin 0.7 for WordPress allows remote attackers to **inject arbitrary web script or HTML** via the v1 parameter.

#### Problem

Based on exploit: <https://www.exploit-db.com/exploits/35067/> The Safe Search plugin for Wordpress is prone to a **cross-site-scripting vulnerability** because it fails to properly sanitize user-supplied input in v1 parameter. An attacker may leverage this issue to **execute arbitrary script** code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to **steal cookie-based authentication credentials and launch other attacks**.

#### Solution

Based on exploit: **sanitize user input**

#### Codes

"Cross-site scripting (XSS)", "Unsanitized data"

---

### CVE-2010-3977

#### Context

**Multiple cross-site scripting (XSS) vulnerabilities** in wp-content/plugins/cforms/lib\_ajax.php in cforms WordPress plugin 11.5 allow remote attackers to **inject arbitrary web script or HTML** via the (1) rs and (2) rsargs[] parameters.

#### Problem

Based on exploit: <https://www.exploit-db.com/exploits/34946/> The cformsII plugin for WordPress is prone to **multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input**. An attacker may leverage these issues to **execute arbitrary**

[script code](#) in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to [steal cookie-based authentication credentials and launch other attacks.](#)

## Solution

Based on exploit: [sanitize user data](#)

## Codes

"Cross-site scripting (XSS)", "Unsanitized data", "improper validation of user-supplied input"

---

## [CVE-2010-2924](#)

### Context

[SQL injection vulnerability](#) in myLDlinker.php in the myLinksDump Plugin 1.2 for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the url parameter.

## Problem

Based on exploit The URL parameter is [not validated properly](#), which enables users to [inject SQL commands](#) through it.

## Solution

Not found

## Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2010-1186](#)

### Context

[Cross-site scripting \(XSS\) vulnerability](#) in xml/media-rss.php in the NextGEN Gallery plugin before 1.5.2 for WordPress allows remote attackers to [inject arbitrary web script or HTML](#) via the mode parameter.

## Problem

Based on exploit. This vulnerability results from reflected [unsanitized input](#) that can be crafted into an attack by a malicious user by manipulating the mode parameter of the xml/media-rss.php script. This vulnerability is triggered because the mode parameter on the media-rss.php script is [not correctly escaped to avoid HTML code injection](#). \$mode = \$\_GET["mode"]; This parameter is reflected back to the user if no correct mode is selected. } else { header('content-type:text/plain; charset=utf-8'); echo sprintf(\_\_("Invalid MediaRSS command (%s).", "nggallery"), \$mode); exit; } It's worth to note that the Content-Type is chosen safely by the plugin, but this is [not enough to avoid code injection](#) because some browsers (most notably Microsoft Internet Explorer) choose the content type by parsing the content the web-server returns instead of obeying the proper headers.

## Solution

Base on exploit: [sanitize data](#)

## Codes

"Unsanitized parameter", "Cross-site scripting (XSS)", "Not escaping characters"

---

## [CVE-2010-0673](#)

### Context

[SQL injection vulnerability](#) in cplphoto.php in the Copperleaf Photolog plugin 0.16, and possibly earlier, for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the postid parameter.

## Problem

The postid parameter is [not validated properly](#), which causes the potential to [inject SQL commands](#) through it.

## Solution

Not found

## Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2009-4748](#)

### Context

[SQL injection vulnerability](#) in mycategoryorder.php in the My Category Order plugin 2.8 and earlier for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the parentId parameter in an act\_OrderCategories action to wp-admin/post-new.php.

## Problem

Based on exploit My Category Order plugin [does not check if the id for a query parameter is integer](#), which enables attackers to [inject SQL commands](#)

## Solution

Based on exploit [Check if the id is integer](#)

## Codes

"SQL injection", "Unrestricted access to database"

---

## [CVE-2009-4672](#)

### Context

[Directory traversal vulnerability](#) in main.php in the WP-Lytebox plugin 1.3 for WordPress allows remote attackers to [include and execute arbitrary local files](#) via a .. (dot dot) in the pg parameter.

## Problem

Based on exploit [Directory traversal can be performed](#) through the pg parameter through '..' which [may give users access to files](#).

## Solution

Not found.

## Codes

"Unsanitized data", "File path traversal"

---

## [CVE-2009-4424](#)

### Context

[SQL injection vulnerability](#) in results.php in the Pyrmont plugin 2 for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the id parameter.

## Problem

Based on exploit The id parameter is [not validated properly](#), which causes the potential for users to [inject SQL commands](#) through it.

## Solution

Base on exploit: [sanitize user input](#)

## Codes

"SQL injection", "Unrestricted access to database"

---

## CVE-2009-2396

### Context

[PHP remote file inclusion vulnerability](#) in template/album.php in DM Albums 1.9.2, as used standalone or as a WordPress plugin, allows remote attackers to [execute arbitrary PHP code](#) via a URL in the SECURITY\_FILE parameter.

### Problem

Based on exploit:

Security File [parameter is not validated properly](#) and can include php files, which causes the potential for [arbitrary code execution](#)

### Solution

Not found

## Codes

"Arbitrary code execution", "Unsanitized parameter"

---

## CVE-2009-2383

### Context

[SQL injection vulnerability](#) in BTE\_RW\_webajax.php in the Related Sites plugin 2.1 for WordPress allows remote attackers to [execute arbitrary SQL commands](#) via the guid parameter.

### Problem

Based on exploit Guid parameter is [not validated properly which enables users to perform SQL Injection](#)

### Solution

Not provided

## Codes

"Sanitize data (enforce expected datatype)", "SQL injection", "Unrestricted access to database"

---

## CVE-2009-2334

### Context

wp-admin/admin.php in WordPress and WordPress MU before 2.8.1 [does not require administrative authentication to access the configuration of a plugin](#), which allows remote attackers to [specify a configuration file in the page parameter to obtain sensitive information or modify this file](#), as demonstrated by the (1) collapsing-archives/options.txt, (2) akismet/readme.txt, (3) related-ways-to-take-action/options.php, (4) wp-security-scan/securityscan.php, and (5) wp-ids/ids-admin.php files. NOTE: this can be [leveraged for cross-site scripting \(XSS\) and denial of service](#).

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/9110/>

A vulnerability was found in the way that WordPress handles some URL requests. This results in [unprivileged users viewing the content of plugins configuration pages](#), and also in some [plugins modifying plugin options](#) and [injecting JavaScript code](#). Arbitrary native code may be run by a malicious attacker if the blog administrator runs injected JavaScript code that edits blog PHP code. No privileges are checked on WordPress plugins configuration PHP modules using parameter 'page' when we replace 'options-general.php' with 'admin.php'. The same thing happens when replacing other modules such as 'plugins.php' with 'admin.php'. Basic information disclosure is done this

way. For example, with the following URL a user with no privileges can see the configuration of plugin Collapsing Archives, if installed.  
[http://\[some\\_wordpress\\_blog\]/wp-admin/admin.php?page=/collapsing-archives/options.txt](http://[some_wordpress_blog]/wp-admin/admin.php?page=/collapsing-archives/options.txt)

## Solution

Not found.

## Codes

"Inject Javascript", "Data leakage", "Lack of security checks"

---

## [CVE-2009-2122](#)

### Context

**SQL injection vulnerability** in viewimg.php in the Paolo Palmonari Photoracer plugin 1.0 for WordPress allows remote attackers to **execute arbitrary SQL commands** via the id parameter.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/8961/> Id parameter in plugin **not validated, which enables users to inject SQL**

## Solution

Not provided

## Codes

"Sanitize data (enforce expected datatype)", "SQL injection", "Unrestricted access to database"

---

## [CVE-2009-0968](#)

### Context

**SQL injection vulnerability** in fmoblog.php in the fMoblog plugin 2.1 for WordPress allows remote attackers to **execute arbitrary SQL commands** via the id parameter to index.php. NOTE: some of these details are obtained from third party information.

### Problem

Based on exploit: <https://www.exploit-db.com/exploits/8229/> Page id parameter is **not validated properly, which enables users to inject SQL using it**

## Solution

Not provided

Based on exploit: **sanitize data**

## Codes

"Unsanitized parameter", "SQL injection", "Unrestricted access to database"

---

## [CVE-2008-6811](#)

### Context

**Unrestricted file upload vulnerability** in image\_processing.php in the e-Commerce Plugin 3.4 and earlier for Wordpress allows remote attackers to **execute arbitrary code by uploading a file with an executable extension**, then accessing it via a direct request to the file in wp-content/plugins/wp-shopping-cart/.

### Problem

An e-Commerce plugin allows to upload executable files and to modify the we-shopping-cart directory which causes the potential for **executing arbitrary code**.

It is possible to upload a selected file to the ... /wp-content/plugins/wp-shopping-cart/ directory. If the directory is not writable (rare cases) you can use the insecure GET variable "imagedir" to **directory traversal so you can upload in different directories**.

## Solution

Not provided.

## Codes

"Remote Code Execution", "Unsanitized data", "File path traversal"

---

## [CVE-2008-5752](#)

### Context

**Directory traversal vulnerability** in getConfig.php in the Page Flip Image Gallery plugin 0.2.2 and earlier for WordPress, when magic\_quotes\_gpc is disabled, allows **remote attackers to read arbitrary files** via a .. (dot dot) in the book\_id parameter. NOTE: some of these details are obtained from third party information.

### Problem

Based on exploit book\_id parameter can be used to **traverse directories** through .. /wp-content/plugins/page-flip-image-gallery/books/getConfig.php?book\_id=../../../../../../../../etc/passwd%00123

## Solution

Not found

## Codes

"File path traversal"

---

## [CVE-2008-5695](#)

### Context

wp-admin/options.php in WordPress MU before 1.3.2, and WordPress 2.3.2 and earlier, **does not properly validate requests** to update an option, which allows remote authenticated users with manage\_options and upload\_files capabilities to **execute arbitrary code by uploading a PHP script** and adding this script's pathname to active\_plugins.

### Problem

WordPress is prone to a vulnerability that lets remote attackers **execute arbitrary code** because the application **fails to sanitize user-supplied input**. Attackers can exploit this issue to **execute arbitrary PHP code within the context of the affected webserver process**.

## Solution

WordPress allows any user with manage\_options capability to **update directly any blog's option** through wp-admin/options.php, so this feature can be used to perform (or hide) multiple attacks where WordPress expects safe data coming from the DB. This bug is very critical in those sites using WordPress MU, because any user has the manage\_options capability.

## Codes

"Arbitrary code execution"

---

## [CVE-2008-4625](#)

### Context

**SQL injection vulnerability** in stnl\_iframe.php in the ShiftThis Newsletter (st\_newsletter) plugin for WordPress allows remote attackers to **execute arbitrary SQL commands** via the newsletter parameter, a different vector than CVE-2008-0683.

#### Problem

Based on exploit The newsletter parameter is **not validated properly**, which causes the potential to **execute arbitrary SQL commands**.

http://flymusic.co.uk/wp-content/plugins/st\_newsletter/stnl\_iframe.php?

newsletter=-9999+UNION+SELECT+concat(user\_login,0x3a,user\_pass,0x3a,user\_email)+FROM+wp\_users--

#### Solution

Not found

Based on Exploit: **sanitize input**

#### Codes

"Sanitize data (enforce expected datatype)", "SQL injection"

---

## CVE-2008-1982

#### Context

**SQL injection vulnerability** in ss\_load.php in the Spreadsheet (wpSS) 0.6 and earlier plugin for WordPress allows remote attackers to **execute arbitrary SQL commands** via the ss\_id parameter.

#### Problem

Based on exploit: <https://www.exploit-db.com/exploits/5486/> The ss\_id **parameter is not checked** if it's an integer and is included in query, which creates the option for **SQL injection**

#### Solution

Not found

Base on exploit: **sanitize input**

#### Codes

"Escape user-supplied data", "Sanitize data (enforce expected datatype)", "SQL injection"

---

## CVE-2008-0491

#### Context

**SQL injection vulnerability** in fim\_rss.php in the fGallery 2.4.1 plugin for WordPress allows remote attackers to **execute arbitrary SQL commands** via the album parameter.

#### Problem

Based on exploit: <https://www.exploit-db.com/exploits/4993/> album **parameter is not escaped or neutralized**.

#### Solution

Not found

Based on exploit: **escape parameter**

#### Codes

"Escape user-supplied data", "SQL injection"

---

## CVE-2007-5800

### **Context**

Only WordPress installations on hosts which allow for register\_globals = on allow\_url\_fopen = on in their php.ini settings are affected.

Multiple [PHP remote file inclusion vulnerabilities](#) in the BackUpWordPress 0.4.2b and earlier plugin for WordPress allow remote attackers to [execute arbitrary PHP code](#) via a URL in the bkpwp\_plugin\_path parameter to (1) plugins/BackUp/Archive.php; and (2) Predicate.php, (3) Writer.php, (4) Reader.php, and other unspecified scripts under plugins/BackUp/Archive/.

### **Problem**

[BASED ON EXPLOIT] The URL parameter is [not validated properly and enables users to execute arbitrary PHP code](#). This is an instance of CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

### **Solution**

Not found

Based on exploit: properly [validate](#) url parameter

### **Codes**

"Arbitrary code execution", "Unsanitized parameter"

---

## CVE-2006-5705

### **Context**

WP-DB-Backup allows the backup of the core WordPress database tables.

[Multiple directory traversal vulnerabilities](#) in plugins/wp-db-backup.php in WordPress before 2.0.5 allow remote authenticated users to [read or overwrite arbitrary files via directory traversal sequences](#) in the (1) backup and (2) fragment parameters in a GET request.

### **Problem**

A [directory traversal](#) can be performed in backup and fragment parameters in GET requests, which enables users to [read or overwrite files through plugins](#). [CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')]

### **Solution**

[Validate backup and fragment parameters](#) to not allow directory traversal. In short, it verifies whether the GET parameters "backup" and "fragment" do not have traversal characters (such as .. or ./ etc)

### **Codes**

"File path traversal", "Lack of sandbox"