



CVE-2008-2800

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-2800
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-07-07 23:41:00 UTC
Updated	2018-10-11 20:43:00 UTC
Description	Mozilla Firefox before 2.0.0.15 and SeaMonkey before 1.1.10 allow remote attackers to bypass the Same Origin Policy and

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	2.0	All	All	All
Application	Mozilla	Firefox	2.0.0.1	All	All	All
Application	Mozilla	Firefox	2.0.0.10	All	All	All
Application	Mozilla	Firefox	2.0.0.11	All	All	All
Application	Mozilla	Firefox	2.0.0.12	All	All	All
Application	Mozilla	Firefox	2.0.0.13	All	All	All
Application	Mozilla	Firefox	2.0.0.2	All	All	All
Application	Mozilla	Firefox	2.0.0.3	All	All	All
Application	Mozilla	Firefox	2.0.0.4	All	All	All
Application	Mozilla	Firefox	2.0.0.5	All	All	All
Application	Mozilla	Firefox	2.0.0.6	All	All	All
Application	Mozilla	Firefox	2.0.0.7	All	All	All
Application	Mozilla	Firefox	2.0.0.8	All	All	All
Application	Mozilla	Firefox	2.0.0.9	All	All	All
Application	Mozilla	Firefox	2.0	All	All	All
Application	Mozilla	Firefox	2.0.0.1	All	All	All
Application	Mozilla	Firefox	2.0.0.10	All	All	All

Application	Mozilla	Firefox	2.0.0.11	All	All	All
Application	Mozilla	Firefox	2.0.0.12	All	All	All
Application	Mozilla	Firefox	2.0.0.13	All	All	All
Application	Mozilla	Firefox	2.0.0.2	All	All	All
Application	Mozilla	Firefox	2.0.0.3	All	All	All
Application	Mozilla	Firefox	2.0.0.4	All	All	All
Application	Mozilla	Firefox	2.0.0.5	All	All	All
Application	Mozilla	Firefox	2.0.0.6	All	All	All
Application	Mozilla	Firefox	2.0.0.7	All	All	All
Application	Mozilla	Firefox	2.0.0.8	All	All	All
Application	Mozilla	Firefox	2.0.0.9	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Seamonkey	1.1	All	All	All
Application	Mozilla	Seamonkey	1.1.2	All	All	All
Application	Mozilla	Seamonkey	1.1.3	All	All	All
Application	Mozilla	Seamonkey	1.1.4	All	All	All
Application	Mozilla	Seamonkey	1.1.5	All	All	All
Application	Mozilla	Seamonkey	1.1.6	All	All	All
Application	Mozilla	Seamonkey	1.1.7	All	All	All
Application	Mozilla	Seamonkey	1.1.8	All	All	All
Application	Mozilla	Seamonkey	1.1	All	All	All
Application	Mozilla	Seamonkey	1.1.2	All	All	All
Application	Mozilla	Seamonkey	1.1.3	All	All	All
Application	Mozilla	Seamonkey	1.1.4	All	All	All
Application	Mozilla	Seamonkey	1.1.5	All	All	All
Application	Mozilla	Seamonkey	1.1.6	All	All	All
Application	Mozilla	Seamonkey	1.1.7	All	All	All
Application	Mozilla	Seamonkey	1.1.8	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All

References

Reference

Red Hat update for seamonkey - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Slackware update for mozilla-firefox - Secunia Advisories - Vulnerability Intelligence - Secunia.com

439035 – Same-origin check in nsXMLHttpRequest::OnChannelRedirect() can be circumvented

Support
Support / Security / Advisories // MDVSA-2008:136 Mandriva
Support
Mozilla Firefox 2.0.0.14 Multiple Remote Vulnerabilities
Repository / Oval Repository
Fedora update for seamonkey - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Fedora update for firefox - Secunia Advisories - Vulnerability Intelligence - Secunia.com
[security-announce] SUSE Security Announcement: Mozilla Firefox (SUSE-SA
The Slackware Linux Project: Slackware Security Advisories
256408
Debian -- Security Information -- DSA-1607-1 iceweasel
[SECURITY] Fedora 8 Update: firefox-2.0.0.15-1.fc8
Red Hat update for thunderbird - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Gentoo update for Mozilla products - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Debian update for iceweasel - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Debian update for xulrunner - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Sun Solaris Firefox Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
[SECURITY] Fedora 8 Update: seamonkey-1.1.10-1.fc8
MFSA 2008-22: XSS through JavaScript same-origin violation
Ubuntu update for firefox - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
432591 – Fix for bug 428672 can be circumvented by using XUL element
Known Vulnerabilities in Mozilla Products
440308 – XSS by using XMLHttpRequest and onreadystatechange handler
Support
Red Hat update for firefox - Secunia Advisories - Vulnerability Intelligence - Secunia.com
wiki.rpath.com/Advisories:rPSA-2008-0216
USN-619-1: Firefox vulnerabilities Ubuntu
Debian -- Security Information -- DSA-1615-1 xulrunner
The Slackware Linux Project: Slackware Security Advisories
428672 – XSS using an event handler attached to the outer window
rhn.redhat.com Red Hat Support
[SECURITY] Fedora 9 Update: seamonkey-1.1.10-1.fc9
Debian update for iceape - Secunia.com
Debian -- Security Information -- DSA-1697-1 iceape
Slackware update for seamonkey - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Mozilla products: Multiple vulnerabilities — Gentoo Linux Documentation
issues.rpath.com/browse/RPL-2646
Webmail - OVH
SUSE update for MozillaFirefox - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Mozilla Firefox 2.0 Has Multiple Bugs That Permit Remote Code Execution, Certificate Spoofing, Cross-Site Scripting, and Other Impacts - SecurityFocus
433328 – XSS using <script> element in unloaded document
Mozilla Firefox Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
rPath update for firefox - Secunia Advisories - Vulnerability Intelligence - Secunia.com
SecurityFocus
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report