



CVE-2007-0800

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

Summary

CVE	CVE-2007-0800
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-07 11:28:00 UTC
Updated	2018-10-16 16:34:00 UTC
Description	Cross-zone vulnerability in Mozilla Firefox 1.5.0.9 considers blocked popups to have an internal zone origin, which allows u

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	1.5.0.9	All	All	All
Application	Mozilla	Firefox	1.5.0.9	All	All	All

References

Reference

Fedora update for firefox - Advisories - Secunia

The Slackware Linux Project: Slackware Security Advisories

SecurityFocus

20070301-01-P

SecurityFocus

Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities

Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Secunia

[rhn.redhat.com](#) | Red Hat Support

Advisories | Mandriva

Repository / Oval Repository

Mozilla Firefox Multiple Vulnerabilities - Advisories - Secunia

[rhn.redhat.com](#) | Red Hat Support

USN-428-1: Firefox vulnerabilities Ubuntu
Mozilla Thunderbird/SeaMonkey/Firefox Multiple Remote Vulnerabilities
issues.rpath.com/browse/RPL-1081
Red Hat update for thunderbird - Advisories - Secunia
Slackware update for seamonkey - Advisories - Secunia
[SECURITY] Fedora Core 5 Update: firefox-1.5.0.10-1.fc5 FedoraNEWS.ORG
Gentoo Linux Documentation -- SeaMonkey: Multiple vulnerabilities
IBM X-Force Exchange
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rPath update for firefox and thunderbird - Advisories - Secunia
[#RPL-1103] thunderbird security update - 1.5.0.10 - rPath Issue Tracking System
HPSBUX02153 SSRT061181 rev.7 - HP-UX Running Firefox, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS)
Webmail - OVH
32108
[Full-disclosure] Firefox + popup blocker + XMLHttpRequest + srand() = oops
SecurityFocus
SUSE update for MozillaFirefox and seamonkey - Advisories - Secunia
MFSA 2007-05: XSS and local file access by opening blocked popups
Mandriva update for firefox - Advisories - Secunia
Mozilla Firefox Popup Blocker Cross Zone Security Bypass Weakness
[Full-disclosure] Firefox + popup blocker + XMLHttpRequest + srand() = oops
Security Announcement
Gentoo update for seamonkey - Advisories - Secunia
Red Hat update for seamonkey - Advisories - Secunia
20070202-01-P
rhn.redhat.com Red Hat Support
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: MozillaFirefox (SUSE-SA:2007:019)
Gentoo update for mozilla-firefox and mozilla-firefox-bin - Advisories - Secunia
rhn.redhat.com Red Hat Support
rhn.redhat.com Red Hat Support
SGI update for seamonkey - Advisories - Secunia
SecurityFocus
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
Fedora update for firefox - Advisories - Secunia
Red Hat update for firefox - Advisories - Secunia

Ubuntu update for firefox - Advisories - Secunia

Mozilla Firefox Flaws Permit Cross-Site Scripting Attacks and Local File Access - SecurityTracker

[SECURITY] Fedora Core 6 Update: firefox-1.5.0.10-1.fc6 | FedoraNEWS.ORG

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](#)