CVE-2007-0778

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-0778
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-26 20:28:00 UTC
Updated	2019-10-09 22:52:00 UTC
Description	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 generat

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All

References

Reference
Fedora update for firefox - Advisories - Secunia
The Slackware Linux Project: Slackware Security Advisories

SecurityFocus

20070301-01-P

Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities

Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Secunia

rhn.redhat.com | Red Hat Support

Advisories | Mandriva

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

Debian update for mozilla-firefox - Advisories - Secunia

Repository / Oval Repository

IBM X-Force Exchange

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

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

rPath update for firefox and thunderbird - Advisories - Secunia

Bug 347852 – reload leaks data from cache to end of page after hash collision in cache

[#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 (Do

Webmail - OVH

MFSA 2007-03: Information disclosure through cache collisions

SUSE update for MozillaFirefox and seamonkey - Advisories - Secunia

Mandriva update for firefox - Advisories - Secunia

Security Announcement

Gentoo update for seamonkey - Advisories - Secunia

Red Hat update for seamonkey - Advisories - Secunia

Mozilla Firefox Cache Collision May Let Remote Users Obtain Cached Web Page Contents - SecurityTracker

Slackware update for mozilla-firefox - Advisories - Secunia

20070202-01-P

The Slackware Linux Project: Slackware Security Advisories

Debian -- Security Information -- DSA-1336-1 mozilla-firefox

[illegible] | Red Hat Support

rhn.redhat.com | Red Hat Support
32110
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
[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.

Free CVE JSON API cve.report/api

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