



CVE-2012-3959

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

Summary

CVE	CVE-2012-3959
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-29 10:56:00 UTC
Updated	2020-08-26 20:36:00 UTC
Description	Use-after-free vulnerability in the nsRangeUpdater::SelAdjDeleteNode function in Mozilla Firefox before 15.0, Firefox ESR

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All

Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All

References			
Reference	Source	Link	Tags
[security-announce] SUSE-SU-2012:1157-1: important: Security update for	SUSE	lists.opensuse.org	Mailing List
Debian -- Security Information -- DSA-2556-1 icedove	DEBIAN	www.debian.org	Third Party
Debian -- Security Information -- DSA-2554-1 iceape	DEBIAN	www.debian.org	Third Party
www.xerox.com/download/security/security-bulletin/16287-4d6b7b0c81f7b/cert_...	CONFIRM	www.xerox.com	Third Party
Malformed Request	BID	www.securityfocus.com	Third Party
[security-announce] openSUSE-SU-2012:1065-1: critical: MozillaFirefox: U	SUSE	lists.opensuse.org	Mailing List
USN-1548-1: Firefox vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Third Party
Repository / Oval Repository	OVAL	oval.cisecurity.org	Third Party
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party
Debian -- Security Information -- DSA-2553-1 iceweasel	DEBIAN	www.debian.org	Third Party
771994 – (CVE-2012-3959) Heap-use-after-free in nsRangeUpdater::SelAdjDeleteNode	CONFIRM	bugzilla.mozilla.org	Issue Track
USN-1548-2: Firefox regression Ubuntu	UBUNTU	www.ubuntu.com	Third Party
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party
MFSA 2012-58: Use-after-free issues found using Address Sanitizer	CONFIRM	www.mozilla.org	Vendor Adv
[security-announce] SUSE-SU-2012:1167-1: important: Security update for	SUSE	lists.opensuse.org	Mailing List
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e
No vendor comments have been submitted for this CVE.			
There are currently no legacy QID mappings associated with this CVE.			

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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