



CVE-2012-5830

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

Summary

CVE	CVE-2012-5830
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-21 12:55:00 UTC
Updated	2020-08-13 17:31:00 UTC
Description	Use-after-free vulnerability in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thund

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	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	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	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	12.10	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	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	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	Suse Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All

Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Application	Suse	Suse Linux Enterprise Software Development Kit	11.0	sp2	All	All
Application	Suse	Suse Linux Enterprise Software Development Kit	11.0	sp2	All	All

References						
Reference			Source		Link	
Security Advisory SA51440 - SUSE update for seamonkey - Secunia			SECUNIA		secunia.com	
Security Advisory SA51359 - Red Hat update for firefox - Secunia			SECUNIA		secunia.com	
Security Advisory SA51434 - SUSE update for xulrunner - Secunia			SECUNIA		secunia.com	
openSUSE-SU-2012:1583-1: moderate: update for MozillaFirefox			SUSE		lists.opensuse.c	
Red Hat Customer Portal			REDHAT		rhn.redhat.com	
openSUSE-SU-2012:1585-1: moderate: update for MozillaThunderbird			SUSE		lists.opensuse.c	
USN-1636-1: Thunderbird vulnerabilities Ubuntu			UBUNTU		www.ubuntu.co	
USN-1638-2: ubufox update Ubuntu			UBUNTU		www.ubuntu.co	
Security Advisory SA51360 - Red Hat update for thunderbird - Secunia			SECUNIA		secunia.com	
87598			OSVDB		osvdb.org	
Red Hat Customer Portal			REDHAT		rhn.redhat.com	
USN-1638-1: Firefox vulnerabilities Ubuntu			UBUNTU		www.ubuntu.co	
About Secunia Research Flexera			SECUNIA		secunia.com	
IBM X-Force Exchange			XF		exchange.xforc	
Access Denied			CONFIRM		bugzilla.mozilla.	
[security-announce] SUSE-SU-2012:1592-1: important: Security update for			SUSE		lists.opensuse.c	
USN-1638-3: Firefox regressions Ubuntu			UBUNTU		www.ubuntu.co	
MFSA 2012-106: Use-after-free, buffer overflow, and memory corruption issues found using Address Sanitizer			CONFIRM		www.mozilla.org	
[security-announce] openSUSE-SU-2013:0175-1: important: security update			SUSE		lists.opensuse.c	
Security Advisory SA51369 - Ubuntu update for firefox - Secunia			SECUNIA		secunia.com	
Security Advisory SA51370 - Ubuntu update for thunderbird - Secunia			SECUNIA		secunia.com	
openSUSE-SU-2012:1586-1: moderate: update for xulrunner			SUSE		lists.opensuse.c	
Security Advisory SA51439 - SUSE update for MozillaFirefox - Secunia			SECUNIA		secunia.com	
CVE Program record			CVE.ORG		www.cve.org	
NVD vulnerability detail			NVD		nvd.nist.gov	

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](#)