



CVE-2013-0776

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

Summary

CVE	CVE-2013-0776
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-19 23:55:00 UTC
Updated	2020-08-06 16:47:00 UTC
Description	Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3

Risk And Classification

Problem Types: CWE-295

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	11.10	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
Operating System	Debian	Debian Linux	7.0	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	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 Aus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Aus	5.9	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	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.9	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 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

References						
Reference			Source	Link	Tags	
USN-1748-1: Thunderbird vulnerabilities Ubuntu			UBUNTU	www.ubuntu.com	Third Party Advisory	
Debian -- Security Information -- DSA-2699-1 iceweasel			DEBIAN	www.debian.org	Third Party Advisory	
Red Hat Customer Portal			REDHAT	rhn.redhat.com	Third Party Advisory	
Access Denied			CONFIRM	bugzilla.mozilla.org	Issue Tracking, Patch, Ven	
USN-1729-1: Firefox vulnerabilities Ubuntu			UBUNTU	www.ubuntu.com	Third Party Advisory	
MSQA-2016-07-21-11: HTTPD 2.4.18.2 - Denial of Service			CONFIRM	httpd.apache.org	Vendor Advisory	

MFSA 2013-27: Phishing on HTTPS connection through malicious proxy	CONFIRM	www.mozilla.org	Vendor Advisory
Repository / Oval Repository	OVAL	oval.cisecurity.org	Third Party Advisory
USN-1729-2: Firefox regression Ubuntu	UBUNTU	www.ubuntu.com	Third Party Advisory
[security-announce] openSUSE-SU-2013:0323-1: important: Mozilla: Februar	SUSE	lists.opensuse.org	Mailing List, Third Party Ad
openSUSE-SU-2013:0324-1: moderate: Mozilla Februarys	SUSE	lists.opensuse.org	Mailing List, Third Party Ad
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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