



CVE-2015-4474

Published on: 08/15/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

CVE-2015-4474

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 40.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

CVE-2015-4474 has been assigned by [m](#) security@mozilla.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Oracle Solaris Bulletin - April 2016

[www.oracle.com](#)
[text/html](#)

[CONFIRM](#)
[www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html](#)

[security-announce] openSUSE-SU-2015:1390-1:
important: Security update

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2015:1390](#)

Mozilla Firefox Multiple Flaws Let Remote Users
Execute Arbitrary Code, Obtain Potentially
Sensitive Information, Bypass Security
Restrictions, and Conduct Cross-Site Scripting
Attacks - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1033247](#)

Access Denied

[bugzilla.mozilla.org](#)
[text/html](#)

[CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1188590](#)

Mozilla Products: Multiple vulnerabilities (GLSA

[security.gentoo.org](#)

[GENTOO GLSA-201605-06](#)

201605-06) — Gentoo security	text/html	
Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1033372
Access Denied	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1181204
USN-2702-2: Ubufox update Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2702-2
[security-announce] SUSE-SU-2015:1528-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1528
USN-2702-1: Firefox vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2702-1
Miscellaneous memory safety hazards (rv:40.0 / rv:38.2) — Mozilla	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2015/mfsa2015-79.html
Access Denied	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1143130
USN-2702-3: Firefox regression Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2702-3
Access Denied	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1161719
Access Denied	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1184068
[security-announce] SUSE-SU-2015:1449-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1449
[security-announce] openSUSE-SU-2015:1389-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1389
[security-announce] SUSE-SU-2015:2081-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2081
Access Denied	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1177501

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

