



CVE-2015-4473

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

Last Modified on: 03/23/2021 11:26:07 PM UTC

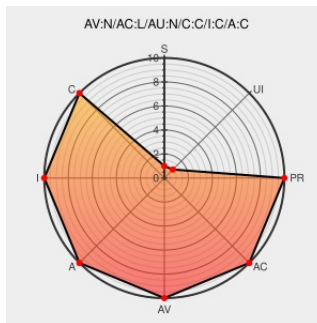
CVE-2015-4473

[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 and Firefox ESR 38.x before 38.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

CVE-2015-4473 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

[Third Party Advisory](#)
[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

[Third Party Advisory](#)
[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

[Third Party Advisory](#)
[VDB Entry](#)
[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1033247](#)

Access Denied

[Issue Tracking](#)

[CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1146213](#)

	Vendor Advisory bugzilla.mozilla.org text/html	
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201605-06
Scheduled Maintenance	Issue Tracking Vendor Advisory bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1178890
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:1586
Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1033372
USN-2702-2: Ubufox update Ubuntu	Broken Link www.ubuntu.com text/html	 UBUNTU USN-2702-2
USN-2712-1: Thunderbird vulnerabilities Ubuntu	Broken Link www.ubuntu.com text/html	 UBUNTU USN-2712-1
[security-announce] SUSE-SU-2015:1528-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2015:1528
openSUSE-SU-2015:1453-1: moderate: Security update for MozillaThunderbir	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1453
Debian -- Security Information -- DSA-3333-1 iceweasel	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-3333
USN-2702-1: Firefox vulnerabilities Ubuntu	Broken Link 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
Debian -- Security Information -- DSA-3410-1 icedove	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-3410
USN-2702-3: Firefox regression Ubuntu	Broken Link www.ubuntu.com text/html	 UBUNTU USN-2702-3
[security-announce] SUSE-SU-2015:1449-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2015:1449
[security-announce] openSUSE-SU-2015:1389-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1389

Access Denied	Issue Tracking Vendor Advisory bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1182711
openSUSE-SU-2015:1454-1: moderate: Security update for MozillaThunderbir	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1454
[security-announce] SUSE-SU-2015:2081-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2015:2081
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:1682

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
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
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All

Application	Mozilla	Firefox Esr	38.0.1	All	All	All
Application	Mozilla	Firefox Esr	38.0.5	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All
Application	Mozilla	Firefox Esr	38.0.1	All	All	All
Application	Mozilla	Firefox Esr	38.0.5	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	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:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:a:mozilla:firefox:***:***:***:						
cpe:2.3:a:mozilla:firefox_esr:38.0:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.0.1:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.0.5:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.1.0:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.0:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.0.1:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.0.5:*****:						

cpe:2.3:a:mozilla:firefox_esr:38.1.0:*****:	
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→