



CVE-2015-7212

Published on: 12/16/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7212

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

Integer overflow in the mozilla::layers::BufferTextureClient::AllocateForSurface function in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allows remote attackers to execute arbitrary code by triggering a graphics operation that requires a large texture allocation.

CVE-2015-7212 has been assigned by [m](#) security@mozilla.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

openSUSE-SU-2015:2353-1: moderate: Security update for MozillaFirefox

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

[SUSE openSUSE-SU-2015:2353](#)

[security-announce] SUSE-SU-2015:2336-1: important: Security update for

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

[SUSE SUSE-SU-2015:2336](#)

Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Same-Origin Policy, and Cause Denial of Service Conditions - SecurityTracker

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

[SECTrack 1034426](#)

Integer overflow allocating extremely large textures — Mozilla

[Vendor Advisory](#)
[www.mozilla.org](#)
[text/html](#)

CONFIRM
[www.mozilla.org/security/announce/2015/mfsa2015-13](#)

[SECURITY] Fedora 23 Update: firefox-43.0-1.fc23	lists.fedoraproject.org text/html	 FEDORA FEDORA-2015-51b1105902
openSUSE-SU-2016:0308-1: moderate: Security update for Seamonkey	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0308
Debian -- Security Information -- DSA-3432-1 icedove	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3432
[security-announce] openSUSE-SU-2015:2380-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2380
USN-2859-1: Thunderbird vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2859-1
Debian -- Security Information -- DSA-3422-1 iceweasel	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3422
[security-announce] SUSE-SU-2015:2335-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:2335
Mozilla Firefox Multiple Security Vulnerabilities	cve.report (archive) text/html	 BID 79279
Oracle Linux Bulletin - October 2015	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbullet2719645.html
Oracle Linux Bulletin - January 2016	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbullet2867209.html
[security-announce] SUSE-SU-2015:2334-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:2334
1222809 - (CVE-2015-7212) Memset crash in mozilla::layers::BufferTextureClient::AllocateForSurface	bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1222809
Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security	security.gentoo.org text/html	 GENTOO GLSA-201512-10
openSUSE-SU-2016:0307-1: moderate: Security update for seamonkey	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0307
[SECURITY] Fedora 22 Update: firefox-43.0-1.fc22	lists.fedoraproject.org text/html	 FEDORA FEDORA-2015-7ab3d3afcf
[security-announce] openSUSE-SU-2015:2406-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2406
USN-2833-1: Firefox vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2833-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:2657

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	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	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	38.1.1	All	All	All
Application	Mozilla	Firefox Esr	38.2.0	All	All	All
Application	Mozilla	Firefox Esr	38.2.1	All	All	All
Application	Mozilla	Firefox Esr	38.3.0	All	All	All
Application	Mozilla	Firefox Esr	38.4.0	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
Application	Mozilla	Firefox Esr	38.1.1	All	All	All
Application	Mozilla	Firefox Esr	38.2.0	All	All	All
Application	Mozilla	Firefox Esr	38.2.1	All	All	All
Application	Mozilla	Firefox Esr	38.3.0	All	All	All
Application	Mozilla	Firefox Esr	38.4.0	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	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

සුභසමුච්ඡි

Operating System	Opensuse	Opensuse	13.2	All	All	All
cpe:2.3:o:fedoraproject:fedora:22:*****:						
cpe:2.3:o:fedoraproject:fedora:23:*****:						
cpe:2.3:o:fedoraproject:fedora:22:*****:						
cpe:2.3:o:fedoraproject:fedora:23:*****:						
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:38.1.1:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.2.0:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.2.1:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.3.0:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.4.0:*****:						
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:a:mozilla:firefox_esr:38.1.1:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.2.0:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.2.1:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.3.0:*****:						
cpe:2.3:a:mozilla:firefox_esr:38.4.0:*****:						
cpe:2.3:o:opensuse:leap:42.1:*****:						
cpe:2.3:o:opensuse:leap:42.1:*****:						
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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)