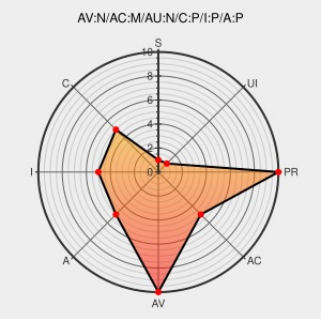
CVE-2015-7222

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

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

CVE-2015-7222

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

Integer underflow in the Metadata::setData function in MetaData.cpp in libstagefright in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allows remote attackers to execute arbitrary code or cause a denial of service (incorrect memory allocation and application crash) via an MP4 video file with crafted covr metadata that triggers a buffer overflow.

CVE-2015-7222 has been assigned by security@mozilla.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	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
[SECURITY] Fedora 23 Update: firefox-43.0-1.fc23	Third Party Advisory lists.fedoraproject.org	FEDORA FEDORA-2015-51b1105902

	text/html	
openSUSE-SU-2016:0308-1: moderate: Security update for Seamonkey	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0308
[security-announce] openSUSE-SU-2015:2380-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2380
Debian -- Security Information -- DSA-3422-1 iceweasel	www.debian.org Depreciated 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/linuxbulletinoct2015-2719645.html
[security-announce] SUSE-SU-2015:2334-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2334
Integer underflow and buffer overflow processing MP4 metadata in libstagefright — Mozilla	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2015/mfsa2015-147.html
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	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0307
1216748 - (CVE-2015-7222) stagefright: potential underflow in 'covr', unchecked allocation© in Metadata::setData	Issue Tracking bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1216748
[SECURITY] Fedora 22 Update: firefox-43.0-1.fc22	Third Party Advisory 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

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
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→