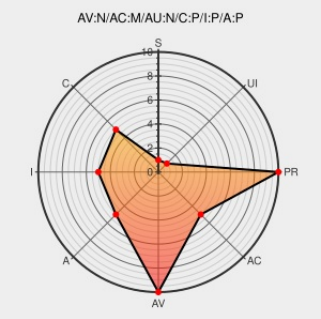
CVE-2015-7189

Published on: 11/04/2015 12:00:00 AM UTC

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

CVE-2015-7189

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

Race condition in the JPEGEncoder function in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow) via vectors involving a CANVAS element and crafted JavaScript code.

CVE-2015-7189 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
Oracle Solaris Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html
1205900 - (CVE-2015-7189) Heap Buffer Overflow in nsJPEGEncoder::ConvertHostARGBRow()	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1205900
[security-announce] SUSE-SU-2015:1978-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1978
openSUSE-SU-2015:2245-1: moderate: Security update for Mozilla Thunderbi	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2245
openSUSE-SU-2015:2229-1: moderate:	lists.opensuse.org	SUSE openSUSE-SU-2015:2229

Security update for Mozilla Thunderbir	text/html	
[security-announce] SUSE-SU-2015:1981-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1981
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2519
[security-announce] SUSE-SU-2015:1926-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:1926
Buffer overflow during image interactions in canvas — Mozilla	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2015/mfsa2015-123.html
Debian -- Security Information -- DSA-3393-1 iceweasel	www.debian.org Depreciated Link text/html	DEBIAN DSA-3393
USN-2819-1: Thunderbird vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2819-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1982
Debian -- Security Information -- DSA-3410-1 icedove	www.debian.org Depreciated Link text/html	DEBIAN DSA-3410
Oracle Linux Bulletin - October 2015	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
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 1034069
Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201512-10
[security-announce] openSUSE-SU-2015:1942-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1942
[security-announce] SUSE-SU-2015:2081-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2081
Mozilla Firefox Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 77411
USN-2785-1: Firefox vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2785-1

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	38.0	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

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:38.0:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→