



CVE-2016-2818

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2016-2818
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-13 10:59:00 UTC
Updated	2023-09-12 14:55:00 UTC
Description	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 all

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

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	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	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	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	45.1.0	All	All	All
Application	Mozilla	Firefox Esr	45.1.1	All	All	All
Application	Mozilla	Firefox Esr	45.1.0	All	All	All
Application	Mozilla	Firefox Esr	45.1.1	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All

Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Application	Novell	Suse Package Hub For Suse Linux Enterprise	12	All	All	All
Application	Novell	Suse Package Hub For Suse Linux Enterprise	12	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
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	5.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	5.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	5.0	All	All	All

Operating System	Redhat	Enterprise Linux For Power Big Endian	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	5.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference

Mozilla Firefox Multiple Security Vulnerabilities

1261230 – be sure to clear stashed views when reconstructing/destroying a subdocument frame

Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Inform

Debian -- Security Information -- DSA-3600-1 firefox-esr

[security-announce] SUSE-SU-2016:1691-1: important: Security update for

1265577 – don't rely on the views we stash when we destroy a subdocument frame to stick around

USN-3023-1: Thunderbird vulnerabilities | Ubuntu

Oracle Linux Bulletin - July 2016

1256493 – hunspell: heap-buffer-overflow write in [@u16_u8]

1264575 – Assertion failure: [barrier verifier] Unmarked edge: object slot, at js/src/gc/Verifier.cpp:301

Debian -- Security Information -- DSA-3647-1 icedove

1256739 – hunspell: stack-buffer-overflow write in [@SfxEntry::checkword]

1234147 – crash in js::jit::JitcodeGlobalTable::allocateTower & js::GetOwnPropertyDescriptor

[security-announce] openSUSE-SU-2016:1557-1: important: Security update

Oracle Linux Bulletin - April 2016

1273701 – pixman image ref-counting races with cairo solid colors

1256968 – hunspell: heap-buffer-overflow write in [@u16_u8]

USN-2993-1: Firefox vulnerabilities | Ubuntu

1261752 – hold strong pointers to view managers and widgets and/or check for destruction in various places

Red Hat Customer Portal

[security-announce] openSUSE-SU-2016:1769-1: important: Security update

[security-announce] openSUSE-SU-2016:1552-1: important: Security update

[security-announce] openSUSE-SU-2016:1778-1: important: Security update

1263384 – VP8 encoder: Heap block overrun (writing) from copy_and_extend_plane -> memset

1269729 – Assertion failure: aIndex < mLength, at dist/include/mozilla/Vector.h:439 with OOM

Red Hat Customer Portal

1273202 – HTMLInputElement may dispatch events inside its destructor

Miscellaneous memory safety hazards (rv:47.0 / rv:45.2) — Mozilla

[security-announce] openSUSE-SU-2016:1767-1: important: Security update

1267130 – nsStandardURL::SetHost called net_ToLowerCase with a bogus pointer, #5

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

690285 Free Berkeley Software Distribution (FreeBSD) Security Update for mozilla (8065d37b-8e7c-4707-a608-1b0a2b8509c3)

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](#)