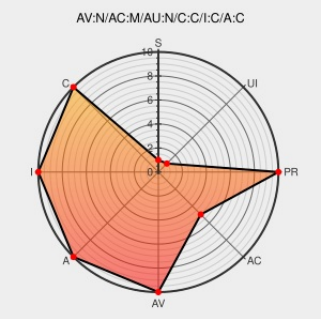
CVE-2014-1519

Published on: 04/30/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-1519

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 29.0 and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

CVE-2014-1519 has been assigned by security@mozilla.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Access Denied	Issue Tracking, Patch, Vendor Advisory, bugzilla.mozilla.org, text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9
Oracle Solaris Bulletin - April 2016	Third Party Advisory, www.oracle.com, text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletina 2952098.html
Access Denied	Issue Tracking, Patch, Vendor Advisory, bugzilla.mozilla.org, text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9
MFSA 2014-34: Miscellaneous memory safety hazards	Vendor Advisory	CONFIRM

(rv:29.0 / rv:24.5)	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2014/mfsa2014-3
Access Denied	Exploit Issue Tracking Patch Vendor Advisory bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9
USN-2185-1: Firefox vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2185-1
Mozilla Seamonkey Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1030164
Access Denied	Exploit Issue Tracking Patch Vendor Advisory bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9
Gentoo Security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201504-01
[SECURITY] Fedora 19 Update: firefox-29.0-5.fc19	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2014-5829
About Secunia Research | Flexera	Third Party Advisory secunia.com Depreciated Link text/plain	SECUNIA 59866
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Conduct Cross-Site Scripting Attacks and Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1030163
openSUSE-SU-2014:0599-1: moderate: update for MozillaFirefox	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0599
996883 – Crash [@ js::jit::Simulator::decodeType2]	Issue Tracking Patch Vendor Advisory bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9
openSUSE-SU-2014:0629-1: moderate: update for seamonkey	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0629
[SECURITY] Fedora 20 Update: thunderbird-24.5.0-1.fc20	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2014-5833
946658 – Intermittent browser_dbg_variables-view-popup-07.js | [@ nsView::DoResetWidgetBounds(bool, bool)] or [@	Issue Tracking Patch Vendor Advisory	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9

nsViewManager::ProcessPendingUpdatesForView(nsView*, bool)]	bugzilla.mozilla.org text/html	
986864 – Crash [@ memmove] or [@ mozilla::PodCopy] or [@ js_NewStringCopyN] or Assertion failure: PointerRangeSize(src, static_cast(dst)) >= nelem, at dist/include/mozilla/PodOperations.h	Issue Tracking Patch Vendor Advisory bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9
953104 – OdinMonkey: Assertion failure: !elems_.empty(), at jit/AsmJS.cpp:1213 or Crash on Heap	Exploit Issue Tracking Patch Vendor Advisory bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=9

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	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Application	Mozilla	Firefox	All	All	All	All

Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:fedoraproject:fedora:19:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:20:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:19:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:20:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:seamonkey:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:seamonkey:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→