

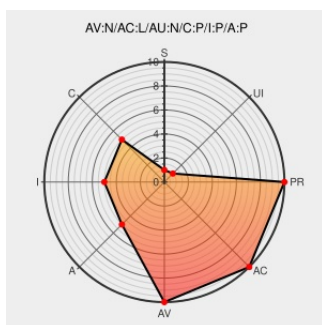


CVE-2013-5619

Published on: 12/11/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:36 PM UTC

CVE-2013-5619

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Multiple integer overflows in the binary-search implementation in SpiderMonkey in Mozilla Firefox before 26.0 and SeaMonkey before 2.23 might allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2013-5619 has been assigned by [m](#) security@mozilla.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Oracle Solaris Bulletin - April 2016

[Third Party Advisory](#)
[www.oracle.com](#)
[text/html](#)

[CONFIRM](#)
[www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html](#)

openSUSE-SU-2014:0008-1: moderate: update for seamonkey

[Mailing List](#)
[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2014:0008](#)

USN-2052-1: Firefox vulnerabilities | Ubuntu

[Third Party Advisory](#)
[www.ubuntu.com](#)
[text/html](#)

[UBUNTU USN-2052-1](#)

[SECURITY] Fedora 20 Update: firefox-26.0-3.fc20

[Mailing List](#)
[Third Party Advisory](#)

[FEDORA FEDORA-2013-23519](#)

	lists.fedoraproject.org text/html	
MFSA 2013-110: Potential overflow in JavaScript binary search algorithms	Vendor Advisory www.mozilla.org text/html	 CONFIRM www.mozilla.org/security/announce/2013/mfsa2013-110.html
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1029470
[security-announce] SUSE-SU-2013:1919-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2013:1919
Gentoo Security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201504-01
Mozilla Seamonkey Multiple Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1029476
917841 – (CVE-2013-5619) binary searches use overflow-prone arithmetic	Issue Tracking Vendor Advisory bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=917841
openSUSE-SU-2013:1918-1: moderate: update for MozillaFirefox	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1918
[SECURITY] Fedora 19 Update: firefox-26.0-2.fc19	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2013-23127
openSUSE-SU-2013:1917-1: moderate: update for MozillaFirefox	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1917
openSUSE-SU-2013:1916-1: moderate: update for MozillaFirefox	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1916

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	Canonical	Ubuntu Linux	12.04	All	All	All

Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	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	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	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	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All

Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	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:13.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:						
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:13.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:						
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:12.2:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:						
cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:						
cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:						

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp3:*:*:*:*:*:vmware:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp3:*:*:*:*:*:vmware:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:11:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:11:sp3:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)