



CVE-2014-1511

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

Summary

CVE	CVE-2014-1511
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-19 10:55:00 UTC
Updated	2020-08-05 14:07:00 UTC
Description	Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via crafted HTML documents, as demonstrated by a crafted HTML document that causes a denial of service (memory consumption) via a crafted HTML document that causes a denial of service (memory consumption).

Risk And Classification

Problem Types: CWE-269

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	12.10	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	13.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox ESR	All	All	All	All
Application	Mozilla	Firefox ESR	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Opensuse	Opensuse	11.4	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	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	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	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.5	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	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	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	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Application	Suse	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Application	Suse	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All

References			
Reference	Source	Link	Tags
Oracle Solaris Bulletin - April 2016	CONFIRM	www.oracle.com	Third Party A
Mozilla Firefox/Thunderbird/SeaMonkey CVE-2014-1511 Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party A
Gentoo Security	GENTOO	security.gentoo.org	Third Party A
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party A
Debian -- Security Information -- DSA-2911-1 icedove	DEBIAN	www.debian.org	Third Party A
MFSA 2014-29: Privilege escalation using WebIDL-implemented APIs	CONFIRM	www.mozilla.org	Vendor Advis
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party A
982909 – (CVE-2014-1511) popup blocker bypass (ZDI-CAN-2215)	CONFIRM	bugzilla.mozilla.org	Exploit, Issue
[security-announce] openSUSE-SU-2014:0584-1: important: MozillaThunderbi	SUSE	lists.opensuse.org	Mailing List, T
Debian -- Security Information -- DSA-2881-1 iceweasel	DEBIAN	www.debian.org	Third Party A
USN-2151-1: Thunderbird vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Third Party A
[security-announce] openSUSE-SU-2014:0448-1: important: MozillaFirefox:	SUSE	lists.opensuse.org	Mailing List, T
[security-announce] SUSE-SU-2014:0418-1: important: Security update for	SUSE	lists.opensuse.org	Mailing List, T
[security-announce] openSUSE-SU-2014:0419-1: important: Mozilla updates	SUSE	lists.opensuse.org	Mailing List, T
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an
No vendor comments have been submitted for this CVE.			
There are currently no legacy QID mappings associated with this CVE.			

© CVE.report 2026 |

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report