



CVE-2014-1531

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

Summary

CVE	CVE-2014-1531
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-30 10:49:00 UTC
Updated	2020-08-07 19:26:00 UTC
Description	Use-after-free vulnerability in the nsGenericHTMLElement::GetWidthHeightForImage function in Mozilla Firefox before 29.0

Risk And Classification

Problem Types: CWE-416

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	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	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
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 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 Server	10	sp4	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All

Operating System	Suse	Suse Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All

References

Reference
Oracle Solaris Bulletin - April 2016
MFSA 2014-44: Use-after-free in imgLoader while resizing images
openSUSE-SU-2014:0640-1: moderate: update for MozillaThunderbird
USN-2185-1: Firefox vulnerabilities Ubuntu
Mozilla Seamonkey Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Conduct Cross-Site Scripting Attacks - Secu
[security-announce] SUSE-SU-2014:0727-1: important: Security update for
openSUSE-SU-2014:0602-1: moderate: Mozilla updates 5/2014
Red Hat Customer Portal
Debian -- Security Information -- DSA-2918-1 iceweasel
[security-announce] SUSE-SU-2014:0665-1: important: Security update for
Gentoo Security
USN-2189-1: Thunderbird vulnerabilities Ubuntu
[SECURITY] Fedora 19 Update: firefox-29.0-5.fc19
About Secunia Research Flexera
Access Denied
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Conduct Cross-Site Scripting Attacks and Local U
Mozilla Firefox/Thunderbird/SeaMonkey CVE-2014-1531 Use After Free Memory Corruption Vulnerability
openSUSE-SU-2014:0599-1: moderate: update for MozillaFirefox
openSUSE-SU-2014:0629-1: moderate: update for seamonkey
Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Conduct Cross-Site Scripting Attacks and L
[SECURITY] Fedora 20 Update: thunderbird-24.5.0-1.fc20
Debian -- Security Information -- DSA-2924-1 icedove
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

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](#)