



# CVE-2014-1482

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

## Summary

<b>CVE</b>	CVE-2014-1482
<b>State</b>	PUBLIC
<b>Assigner</b>	security@mozilla.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-02-06 05:44:00 UTC
<b>Updated</b>	2020-08-11 13:33:00 UTC
<b>Description</b>	RasterImage.cpp in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey be

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	13.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	13.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	19	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	19	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Seamonkey</a>	All	All	All	All

Application	<a href="#">Mozilla</a>	<a href="#">Seamonkey</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Thunderbird</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Thunderbird</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Desktop</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Desktop</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	11	sp3	All	All

Application	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	11.0	sp3	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	11.0	sp3	All	All

## References

### Reference

[Security Advisory SA56761 - Red Hat update for firefox - Secunia](#)

[Oracle Solaris Bulletin - April 2016](#)

[Security Advisory SA56706 - Cyberfox Multiple Vulnerabilities - Secunia](#)

[Debian -- Security Information -- DSA-2858-1 iceweasel](#)

[Security Advisory SA56787 - Mozilla Firefox Multiple Vulnerabilities - Secunia](#)

[Mozilla Thunderbird Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker](#)

[\[security-announce\] openSUSE-SU-2014:0212-1: important: Mozilla Firefox](#)

[102868](#)

[\[SECURITY\] Fedora 20 Update: thunderbird-24.3.0-1.fc20](#)

[Security Advisory SA56858 - Debian update for iceweasel - Secunia](#)

[Gentoo Security](#)

[8pecxstudios.com](#)

[USN-2102-1: Firefox vulnerabilities | Ubuntu](#)

[Security Advisory SA56888 - Ubuntu update for firefox - Secunia](#)

[\[SECURITY\] Fedora 19 Update: thunderbird-24.3.0-1.fc19](#)

[Red Hat Customer Portal](#)

[USN-2119-1: Thunderbird vulnerabilities | Ubuntu](#)

[Security Advisory SA56767 - Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities - Secunia](#)

[Mozilla Firefox/Thunderbird/SeaMonkey CVE-2014-1482 Remote Code Execution Vulnerability](#)

[Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker](#)

[943803 – \(CVE-2014-1482\) Image decoding causing FireFox to crash with Goo Create](#)

[\[security-announce\] SUSE-SU-2014:0248-1: important: Security update for](#)

[IBM X-Force Exchange](#)

[Red Hat Customer Portal](#)

[MFSA 2014-04: Incorrect use of discarded images by RasterImage](#)

[Downloads](#)

[USN-2102-2: Firefox regression | Ubuntu](#)

[\[security-announce\] openSUSE-SU-2014:0213-1: important: Mozilla updates](#)

[download.novell.com/Download](#)

[\[security-announce\] openSUSE-SU-2014:0419-1: important: Mozilla updates](#)

[Security Advisory SA56763 - Red Hat update for thunderbird - Secunia](#)

Security Advisory SA56922 - SUSE update for Multiple Mozilla Packages - Secunia

Mozilla Seamonkey Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)