



CVE-2015-0818

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-0818
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-24 00:59:00 UTC
Updated	2016-12-22 02:59:00 UTC
Description	Mozilla Firefox before 36.0.4, Firefox ESR 31.x before 31.5.3, and SeaMonkey before 2.33.1 allow remote attackers to byp

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	31.0	All	All	All
Application	Mozilla	Firefox Esr	31.1	All	All	All
Application	Mozilla	Firefox Esr	31.1.0	All	All	All
Application	Mozilla	Firefox Esr	31.1.1	All	All	All
Application	Mozilla	Firefox Esr	31.2	All	All	All
Application	Mozilla	Firefox Esr	31.3	All	All	All
Application	Mozilla	Firefox Esr	31.3.0	All	All	All
Application	Mozilla	Firefox Esr	31.4	All	All	All
Application	Mozilla	Firefox Esr	31.5	All	All	All
Application	Mozilla	Firefox Esr	31.5.1	All	All	All
Application	Mozilla	Firefox Esr	31.5.2	All	All	All
Application	Mozilla	Firefox Esr	31.0	All	All	All
Application	Mozilla	Firefox Esr	31.1	All	All	All
Application	Mozilla	Firefox Esr	31.1.0	All	All	All
Application	Mozilla	Firefox Esr	31.1.1	All	All	All
Application	Mozilla	Firefox Esr	31.2	All	All	All

Application	Mozilla	Firefox Esr	31.3	All	All	All
Application	Mozilla	Firefox Esr	31.3.0	All	All	All
Application	Mozilla	Firefox Esr	31.4	All	All	All
Application	Mozilla	Firefox Esr	31.5	All	All	All
Application	Mozilla	Firefox Esr	31.5.1	All	All	All
Application	Mozilla	Firefox Esr	31.5.2	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All

References

Reference

[Red Hat Customer Portal](#)

[openSUSE-SU-2015:0636-1: important: Security update for seamonkey](#)

[Gentoo Security](#)

[USN-2538-1: Firefox vulnerabilities | Ubuntu](#)

[Debian -- Security Information -- DSA-3201-1 iceweasel](#)

[Mozilla Firefox SVG Processing Flaw Lets Remote Users Bypass Same-Origin Policy and Execute Arbitrary Scripts with Elevated Privileges -](#)

[Privilege escalation through SVG navigation — Mozilla](#)

[Mozilla Firefox/SeaMonkey CVE-2015-0818 Privilege Escalation Vulnerability](#)

[Access Denied](#)

[\[security-announce\] openSUSE-SU-2015:0567-1: important: update to Firefo](#)

[\[security-announce\] SUSE-SU-2015:0630-1: important: Security update for](#)

[\[security-announce\] SUSE-SU-2015:0593-1: important: Security update for](#)

[Oracle Solaris Third Party Bulletin - April 2015](#)

[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](#).

