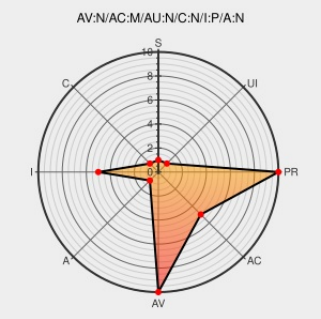
CVE-2015-4518

Published on: 11/04/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

CVE-2015-4518

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firefox from Mozilla contain the following vulnerability:

The Reader View implementation in Mozilla Firefox before 42.0 has an improper whitelist, which makes it easier for remote attackers to bypass the Content Security Policy (CSP) protection mechanism and conduct cross-site scripting (XSS) attacks via vectors involving SVG animations and the about:reader URL.

CVE-2015-4518 has been assigned by security@mozilla.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Oracle Solaris Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html
CSP bypass due to permissive Reader mode whitelist — Mozilla	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2015/mfsa2015-118.html
1182778 - (CVE-2015-4518) Passive script execution on about:reader via SVG animations (affects: Firefox, NoScript, CSP; impact: spoofing, phishing)	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1182778
1136692 - Reader Mode does not completely disable all active content (XSS)	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1136692

Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restrictions, and Conduct Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034069
Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201512-10
[security-announce] openSUSE-SU-2015:1942-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1942
USN-2785-1: Firefox vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2785-1

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
Application	Mozilla	Firefox	All	All	All	All

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→