

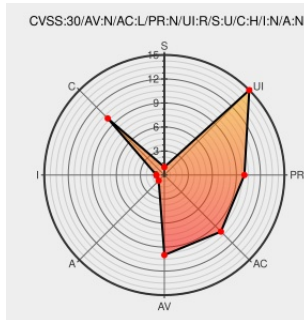


CVE-2016-1967

Published on: 03/13/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:05 PM UTC

CVE-2016-1967

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Firefox](#) from [Mozilla](#) contain the following vulnerability:

Mozilla Firefox before 45.0 does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via crafted JavaScript code that leverages history.back and performance.getEntries calls after restoring a browser session. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-7207.

CVE-2016-1967 has been assigned by [m](#) security@mozilla.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
USN-2917-3: Firefox regressions Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2917-3

Same-origin policy violation using performance.getEntries and history navigation with session restore — Mozilla	Vendor Advisory www.mozilla.org text/html	 CONFIRM www.mozilla.org/security/announce/2016/mfsa2016-29.html
USN-2917-1: Firefox vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2917-1
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201605-06
[security-announce] openSUSE-SU-2016:0733-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0733
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Spoof the Address Bar, Overwrite Files, and Deny Service - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1035215
[security-announce] openSUSE-SU-2016:0731-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0731
USN-2917-2: Firefox regressions Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2917-2
Access Denied	bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1246956

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 →](#)

© CVE.report 2023   |

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](#)