



CVE-2016-1949

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

Summary

CVE	CVE-2016-1949
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-13 02:59:00 UTC
Updated	2016-12-06 03:07:00 UTC
Description	Mozilla Firefox before 44.0.2 does not properly restrict the interaction between Service Workers and plugins, which allows r

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

References

Reference	Source
openSUSE-SU-2016:0553-1: moderate: Security update for Mozilla Firefox	SL
1245724 - (CVE-2016-1949) NPAPI-initiated network requests can be intercepted by service workers breaking plugin origin expectations	CC
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security	GL
openSUSE-SU-2016:0489-1: moderate: Security update for MozillaFirefox	SL
Same-origin-policy violation using Service Workers with plugins — Mozilla	CC
Mozilla Firefox Plugin Request Processing Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker	SE
USN-2893-1: Firefox vulnerability Ubuntu	UF
CVE Program record	CV
NVD vulnerability detail	NV

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](#)