CVE-2015-4490

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-4490
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-16 01:59:18 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The nsCSPHostSrc::permits function in dom/security/nsCSPUtils.cpp in Mozilla Firefox before 40.0 does not implement the

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All

Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
USN-2702-1: Firefox vulnerabilities | Ubuntu
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restriction
USN-2702-2: Ubufox update | Ubuntu
[security-announce] openSUSE-SU-2015:1389-1: important: Security update
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security
Mozilla Content Security Policy allows for asterisk wildcards in violation of CSP specification — Mozilla
[security-announce] openSUSE-SU-2015:1390-1: important: Security update
1086999 – (CVE-2015-4490) CSP: Asterisk (*) wildcard should not allow blob:, data:, or filesystem: when matching source expressions
USN-2702-3: Firefox regression | Ubuntu
Oracle Solaris Bulletin - April 2016
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 and Source URL Uptime Status status.cve.report