CVE-2015-7218

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

Summary

CVE	CVE-2015-7218
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-16 11:59:16 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The HTTP/2 implementation in Mozilla Firefox before 43.0 allows remote attackers to cause a denial of service (integer und

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	22	All	All	All

Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

Vendor Declared Affected Products

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

References

Reference
[SECURITY] Fedora 22 Update: firefox-43.0-1.fc22
Mozilla Firefox Multiple Security Vulnerabilities
openSUSE-SU-2015:2353-1: moderate: Security update for MozillaFirefox
openSUSE-SU-2016:0308-1: moderate: Security update for Seamonkey
Access Denied
[SECURITY] Fedora 23 Update: firefox-43.0-1.fc23
openSUSE-SU-2016:0307-1: moderate: Security update for seamonkey
USN-2833-1: Firefox vulnerabilities | Ubuntu
DOS due to malformed frames in HTTP/2 — Mozilla
Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Same-Origin Policy
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report