CVE-2014-1485

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

Summary

CVE	CVE-2014-1485
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-06 05:44:24 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The Content Security Policy (CSP) implementation in Mozilla Firefox before 27.0 and SeaMonkey before 2.24 operates on X

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

EPSS: 0.009640000 probability, percentile 0.766050000 (date 2026-05-04)

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

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	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All

Vendor Declared Affected Products

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

References

Reference
[security-announce] SUSE-SU-2014:0248-1: important: Security update for
Gentoo Security
Security Advisory SA56706 - Cyberfox Multiple Vulnerabilities - Secunia
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker
Mozilla Firefox/SeaMonkey CVE-2014-1485 Cross Site Scripting Vulnerability
910139 – (CVE-2014-1485) CSP should block XSLT as script, not as style
Security Advisory SA56888 - Ubuntu update for firefox - Secunia
Mozilla Seamonkey Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker
IBM X-Force Exchange
8pecxstudios.com
Security Advisory SA56767 - Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities - Secunia
[security-announce] openSUSE-SU-2014:0212-1: important: Mozilla Firefox
USN-2102-2: Firefox regression | Ubuntu
osvdb.org/102871
[security-announce] openSUSE-SU-2014:0419-1: important: Mozilla updates
MFSA 2014-07: XSLT stylesheets treated as styles in Content Security Policy

Security Advisory SA56787 - Mozilla Firefox Multiple Vulnerabilities - Secunia
USN-2102-1: Firefox vulnerabilities | 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.