CVE-2015-1284

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

Summary

CVE	CVE-2015-1284
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-23 00:59:13 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The LocalFrame::isURLAllowed function in core/frame/LocalFrame.cpp in Blink, as used in Google Chrome before 44.0.240

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

Problem Types: CWE-20 | 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
Application	Google	Chrome	All	All	All	All

Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.7.z	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	6.0	All	All	All

Vendor Declared Affected Products

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

References

Reference
[blink] Revision 197139
Red Hat Customer Portal
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Infor
Chrome Releases: Stable Channel Update
[security-announce] openSUSE-SU-2015:1287-1: important: Security update
Google Chrome Prior to 44.0.2403.89 Multiple Security Vulnerabilities
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security
Issue 493243 - chromium - Heap-use-after-free in blink::Frame::deprecatedLocalOwner - An open-source project to help move the web forwar
Debian -- Security Information -- DSA-3315-1 chromium-browser
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.