CVE-2015-1267

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

Summary

CVE	CVE-2015-1267
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-26 14:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Blink, as used in Google Chrome before 43.0.2357.130, does not properly restrict the creation context during creation of a D

Risk And Classification

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

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

Problem Types: CWE-254 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Red Hat Customer Portal
openSUSE-SU-2015:1872-1: moderate: Security update for chromium
[blink] Revision 196755
Chrome Releases: Chrome Stable Update
openSUSE-SU-2015:1146-1: moderate: Security update for chromium
Google Chrome CVE-2015-1267 Cross-Origin Security Bypass Vulnerability
Gentoo Security
Issue 1174343003: blink:bindings: Passes the global context instead of |this| in JS. - Code Review
Debian -- Security Information -- DSA-3315-1 chromium-browser
Issue 497507 - chromium - Security: Cross-origin scripting possible via native functions - An open-source project to help move the web forwar
USN-2652-1: Oxide vulnerabilities | Ubuntu
Google Chrome Bugs Let Remote Users Bypass Same-Origin Restrictions - SecurityTracker
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.