CVE-2015-1293

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

Summary

CVE	CVE-2015-1293
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-03 22:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The DOM implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the S

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-264 | 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

Vendor Declared Affected Products

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

References

Reference
Debian -- Security Information -- DSA-3351-1 chromium-browser
openSUSE-SU-2015:1873-1: moderate: Security update for Chromium
Chrome Releases: Stable Channel Update
Red Hat Customer Portal
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, Obtain Potentially Sensitive Informatic
Issue 524074 - chromium - Security: Universal XSS by loading a javascript: URI from an unloaded window - Monorail
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security
openSUSE-SU-2015:1586-1: moderate: Security update for Chromium
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.