CVE-2015-6766

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

Summary

CVE	CVE-2015-6766
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-06 01:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Use-after-free vulnerability in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attacker

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: NVD-CWE-Other | 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
[security-announce] openSUSE-SU-2015:2290-1: important: Security update
USN-2825-1: Oxide vulnerabilities | Ubuntu
Chrome Releases: Stable Channel Update
Issue 1418783005: Fix possible map::end() dereference in AppCacheUpdateJob triggered by a compromised renderer. - Code Review
Google Chrome Prior to 47.0.2526.73 Multiple Security Vulnerabilities
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security
[security-announce] openSUSE-SU-2015:2291-1: important: Security update
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Spoof Content - SecurityTracker
Sign in - Google Accounts
Debian -- Security Information -- DSA-3415-1 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.