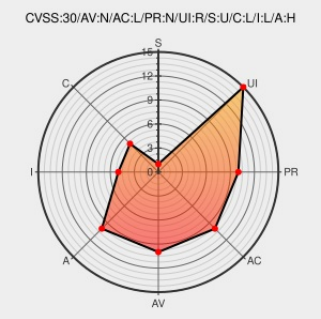
CVE-2016-1612

Published on: 01/25/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

CVE-2016-1612

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Chrome from Google contain the following vulnerability:

The LoadIC::UpdateCaches function in ic/ic.cc in Google V8, as used in Google Chrome before 48.0.2564.82, does not ensure receiver compatibility before performing a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact via crafted JavaScript code.

CVE-2016-1612 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2016:0249-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0249
497632 - chromium - An open-source project to	code.google.com	CONFIRM code.google.com/p/chromium/issues/det

help move the web forward. - Monorail	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/det
Chrome Releases: Stable Channel Update	Patch Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/201 update_20.html
[security-announce] openSUSE-SU-2016:0271-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0271
[security-announce] openSUSE-SU-2016:0250-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0250
Debian -- Security Information -- DSA-3456-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3456
cfbd16172fa165cc33ce0e2e72f74e5561168a61 - v8/v8 - Git at Google	chromium.googlesource.com text/html	CONFIRM chromium.googlesource.com/v8/v8/+/cfbd16172fa165c
USN-2877-1: Oxide vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2877-1
Google Chrome Multiple Bugs Let Remote Users Obtain Information, Bypass Security Restrictions, Spoof URLs, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034801
Issue 1531583005: [IC] Fix "compatible receiver" checks hidden behind interceptors - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1531583005
Google V8 Prior to 4.8.271.17 Multiple Unspecified Security Vulnerabilities	cve.report (archive) text/html	BID 81431
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0072
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201603-09

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→