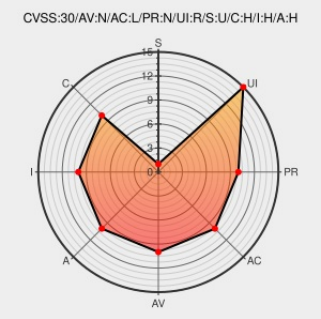
CVE-2016-1641

Published on: 03/05/2016 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:30:00 AM UTC

CVE-2016-1641

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



Certain versions of Chrome from Google contain the following vulnerability:

Use-after-free vulnerability in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an image download after a certain data structure is deleted, as demonstrated by a favicon.ico download.

CVE-2016-1641 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2016:0684-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0684

Google Chrome Prior to 49.0.2623.75 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 84008
USN-2920-1: Oxide vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2920-1
[security-announce] openSUSE-SU-2016:0664-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0664
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201603-09
Debian -- Security Information -- DSA-3507-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3507
Issue 1730363003: Don't call WebContents::DownloadImage() callback if the WebContents were deleted - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1730363003
583718 - Heap-use-after-free in favicon::FaviconDriverImpl::DidDownloadFavicon - chromium - Monorail	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=583718
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Information - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1035185
[security-announce] openSUSE-SU-2016:0729-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0729
[security-announce] SUSE-SU-2016:0665-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0665
Chrome Releases: Stable Channel Update	googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/03/stable-channel-update.html

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→

CVE.report and Source URL Uptime Status status.cve.report