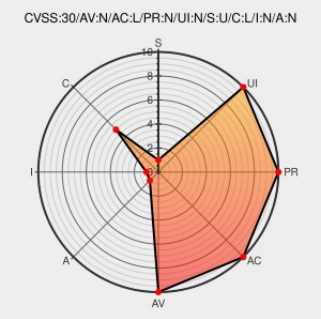
CVE-2016-2845

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

Last Modified on: 11/07/2023 02:32:00 AM UTC

CVE-2016-2845

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



Certain versions of Chrome from Google contain the following vulnerability:

The Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 49.0.2623.75, does not ignore a URL's path component in the case of a ServiceWorker fetch, which allows remote attackers to obtain sensitive information about visited web pages by reading CSP violation reports, related to FrameFetchContext.cpp and ResourceFetcher.cpp.

CVE-2016-2845 has been assigned by security@google.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
USN-2920-1: Oxide vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2920-1

591402 - Tracking bug for internal fixes: Chrome M49, release 0 - chromium - Monorail	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=591402
Egor Homakov: Using Content-Security-Policy for Evil	homakov.blogspot.com text/html	MISC homakov.blogspot.com/2014/01/using-content-security-policy-for-evil.html
Google Chrome CVE-2016-2845 Information Disclosure Vulnerability	cve.report (archive) text/html	BID 84168
542060 - chromium - An open-source project to help move the web forward. - Monorail	bugs.chromium.org text/html	CONFIRM bugs.chromium.org/p/chromium/issues/detail?id=542060
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
Issue 1454003003: [CSP] Don't check the path component of the URL when the response was fetched via ServiceWorker. - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1454003003/
Chrome Releases: Stable Channel Update	googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/03/stable-channel-update.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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→