



CVE-2015-1292

Published on: 09/03/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1292

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

The NavigatorServiceWorker::serviceWorker function in modules/serviceworkers/NavigatorServiceWorker.cpp in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy by accessing a Service Worker.

CVE-2015-1292 has been assigned by security@google.com to track the vulnerability

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

Chrome Releases: Stable Channel Update

[Patch](#)
[Vendor Advisory](#)
[googlechromereleases.blogspot.com](#)
[text/html](#)

CONFIRM
[googlechromereleases.blogspot.com/2015/09/stable-channel-update.html](#)

Issue 522791 - chromium - Security: Universal XSS using navigator.serviceWorker.ready - Monorail

[code.google.com](#)
[text/html](#)

CONFIRM
[code.google.com/p/chromium/issues/detail?id=522791](#)

Issue 1307883002: Add cross origin access check to navigator.serviceWorker. - Code Review

[codereview.chromium.org](#)
[text/html](#)

CONFIRM
[codereview.chromium.org/1307883002/](#)

Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, Obtain Potentially Sensitive Information, and Spoof Content -

[www.securitytracker.com](#)
[text/html](#)

SECTRAK 1033472

Information, and Open Content

SecurityTracker

openSUSE-SU-2015:1873-1: moderate: Security update for Chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1873
[blink] Revision 201055	src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/blink?revision=201055&view=revision
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201603-09
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1712
openSUSE-SU-2015:1586-1: moderate: Security update for Chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1586
Debian -- Security Information -- DSA-3351-1 chromium-browser	www.debian.org Deprecated Link text/html	DEBIAN DSA-3351

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