

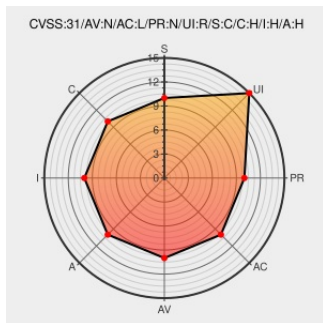


CVE-2020-16017

Published on: 01/08/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:49 PM UTC

CVE-2020-16017

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Use after free in site isolation in Google Chrome prior to 86.0.4240.198 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

CVE-2020-16017 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Google - Chrome** version < 86.0.4240.198

CVSS3 Score: **9.6 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	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
1146709 - chromium - An open-source project to help move the web forward. - Monorail	Permissions Required Vendor Advisory	MISC crbug.com/1146709

Vendor Release

crbug.com

text/html

Chrome Releases: Stable Channel Update for Desktop

Release Notes

Vendor Advisory

chromereleases.googleblog.com

text/html

MISC

chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_11.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.

Related QID Numbers

750514 OpenSUSE Security Update for opera (openSUSE-SU-2020:2178-1)

750596 OpenSUSE Security Update for chromium (openSUSE-SU-2020:1929-1)

983064 Dotnet (nuget) Security Update for CefSharp.Wpf.HwndHost (GHSA-gvqv-779r-4jgp)

Known Affected Configurations (CPE V2.3)

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →