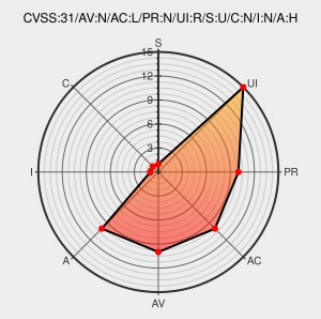
CVE-2019-5825

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 10/07/2022 06:57:00 PM UTC

CVE-2019-5825

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



Certain versions of Chrome from Google contain the following vulnerability:

Out of bounds write in JavaScript in Google Chrome prior to 73.0.3683.86 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2019-5825 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 73.0.3683.86**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Chrome Releases: Stable Channel Update for Desktop	Release Notes Vendor Advisory	MISC chromereleases.googleblog.com/2019/04/stable-

	chromereleases.googleblog.com text/html	channel-update-for-desktop_30.html
Issue 941743 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Patch Third Party Advisory crbug.com text/html	MISC crbug.com/941743
Google Chrome 72 / 73 Array.map Corruption ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/156641/Google-Chrome-72-73-Array.map-Corruption.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
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→