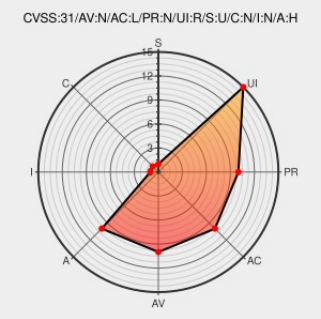
CVE-2019-5826

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

Last Modified on: 03/23/2021 11:27:59 PM UTC

CVE-2019-5826

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



Certain versions of Chrome from Google contain the following vulnerability:

Use after free in IndexedDB in Google Chrome prior to 73.0.3683.86 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.

CVE-2019-5826 has been assigned by security@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 chromereleases.googleblog.com	MISC chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop_30.html

	text/html	
Issue 941746 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Patch Third Party Advisory crbug.com text/html	MISC crbug.com/941746

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→