

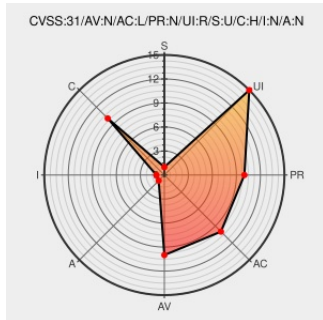


CVE-2020-6503

Published on: 06/03/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-6503

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

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

Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.

CVE-2020-6503 has been assigned by [chrome-cve-admin@google.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Google](#) - **Chrome** version < 74.0.3729.108

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	HIGH	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

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

[channel-update-for-desktop_23.html](#)

text/html

comment@cve.report.

Known Affected Configurations (CPE V2.3)

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

Next ID→