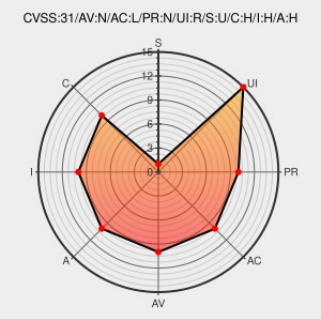
CVE-2020-6507

Published on: 07/22/2020 12:00:00 AM UTC

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

CVE-2020-6507

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



Certain versions of Chrome from Google contain the following vulnerability:

Out of bounds write in V8 in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6507 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 83.0.4103.106**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	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
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202007-08) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202007-08

1086890 - chromium - An open-source project to help move the web forward. - Monorail	Issue Tracking Permissions Required Third Party Advisory crbug.com text/html	MISC crbug.com/1086890
Google Chrome 81.0.4044 V8 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162088/Google-Chrome-81.0.4044-V8-Remote-Code-Execution.html
Chrome Releases: Stable Channel Update for Desktop	Vendor Advisory chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_15.html
Google Chrome 81.0.4044 V8 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162105/Google-Chrome-81.0.4044-V8-Remote-Code-Execution.html

Related QID Numbers

500849 Alpine Linux Security Update for chromium

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

Social Mentions

Source	Title	Posted (UTC)
@ipssignatures	It's new to me that CheckPoint has a protection/signature/rule for the vulnerability CVE-2020-6507.... twitter.com/i/web/status/1…	2021-03-31 11:02:01
@ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-6507. #Szx5txhh3e6af4	2021-03-31 11:02:01
@BlogLoki	【PoC】CVE-2020-6507、CVE-2020-16040 久しく見なかったChromeのPoCです。RCEです。・CVE-2020-6507 exploit-db.com/exploits/49746 ・CVE-2020-16… twitter.com/i/web/status/1…	2021-04-06 11:15:55
@buaqbot	从 0 开始学 V8 漏洞利用之 CVE-2020-6507（四） ift.tt/tLeUVpo ift.tt/gOC2uKD	2022-02-04 02:07:14
@buaqbot	从 0 开始学 V8 漏洞利用之 CVE-2020-6507（四） ift.tt/7dhiTy1 ift.tt/Rw8X9t1	2022-02-04 05:29:40

@brandon_shi	Browser Exploitation: A Case Study Of CVE-2020-6507 y4y.space/2022/08/05/bro…	2022-08-05 09:12:30
@d34dr4bbit	Browser Exploitation: A Case Study Of CVE-2020-6507 – ! aeternusmalus.wordpress.com/2022/08/05/bro…	2022-08-05 14:25:39
@ipssignatures	The vuln CVE-2020-6507 has a tweet created 0 days ago and retweeted 13 times. twitter.com/brandon_shi/st… #pow1rtrtwwcve	2022-08-05 16:06:01
@MariaRusanova88	Browser Exploitation: A Case Study Of CVE-2020-6507 – ! The most browser exploitation scenarios consists of multipl… twitter.com/i/web/status/1…	2022-08-06 12:45:21
@01_security_01	Browser Exploitation: A Case Study Of CVE-2020-6507 - y4y.space/2022/08/05/bro… #0day #cyberthreat #backdoor	2022-08-07 13:03:15

← Previous ID

Next ID→