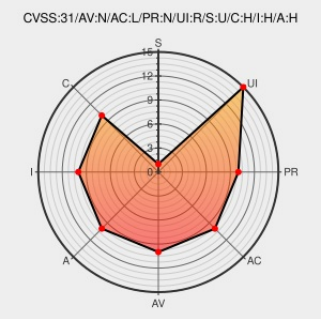
CVE-2021-38001

Published on: 11/23/2021 12:00:00 AM UTC

Last Modified on: 11/24/2021 04:28:00 PM UTC

CVE-2021-38001

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Chrome from Google contain the following vulnerability:

Type confusion in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-38001 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 95.0.4638.69**

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
Chrome Releases: Stable Channel Update for Desktop	chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2021/10/stable-

		channel-update-for-desktop_28.html
1260577 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/1260577

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

376000 Google Chrome Prior to 95.0.4638.69 Multiple Vulnerabilities

376010 Microsoft Edge Based on Chromium Prior to 95.0.1020.40 Multiple Vulnerabilities

690221 Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (976d7bf9-38ea-11ec-b3b0-3065ec8fd3ec)

751335 OpenSUSE Security Update for chromium (openSUSE-SU-2021:1462-1)

Known Affected Configurations (CPE V2.3)

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@haeretics	8件の脆弱性に対処。「CVE-2021-38000」と「CVE-2021-38003」はすでに悪用を確認。「CVE-2021-38001」「CVE-2021-38002」は中国のハッキングコンテスト「天府杯」で報告され、すでに攻撃… twitter.com/i/web/status/1…	2021-10-29 02:15:04
@P4nda20371774	Reproduced the V8 bug (CVE-2021-38001) used by KunlunLab at TianfuCup 2021. Really nice find. https://t.co/9hfqDp2XCU	2021-11-03 11:53:12
@ipssignatures	The vuln CVE-2021-38001 has a tweet created 0 days ago and retweeted 10 times. twitter.com/P4nda20371774/… #pow1rtrtwwcve	2021-11-04 06:06:00
@ma1fan	Here is the #TianfuCup 2021 chrome v8 bug CVE-2021-38001 poc write by myself , Enjoy it :) github.com/maldiohead/TFC…	2021-11-05 03:15:17
@piedpiper1616	GitHub - maldiohead/TFC-Chrome-v8-bug-CVE-2021-38001-poc - github.com/maldiohead/TFC…	2021-11-05 05:26:15
@vngkv123	Sorry for re-upload. CVE-2021-38001 V8 POC exploit about @s0rrymybad of Kunlun Lab via Tianfu Cup 2021. github.com/vngkv123/aSiag…	2021-11-05 07:45:06
@ipssignatures	The vuln CVE-2021-38001 has a tweet created 0 days ago and retweeted 15 times. twitter.com/vngkv123/statu… #pow1rtrtwwcve	2021-11-05 12:06:00
@sploitus_com	Exploit for CVE-2021-38001 sploitus.com/exploit?id=E86… #Exploit #Sploitus	2021-11-06 00:25:21
@vngkv123	Simple writeup for CVE-2021-38001 (Chrome V8). If you find some wrong things, plz let me know =] github.com/vngkv123/artic…	2021-11-06 13:37:28

@ipssignatures	The vuln CVE-2021-38001 has a tweet created 0 days ago and retweeted 19 times. twitter.com/vngkv123/statu… #pow1rtrtwwcve	2021-11-06 18:06:01
@Har_sia	CVE-2021-38001 har-sia.info/CVE-2021-38001… #HarsiaInfo	2021-11-07 23:01:03
@CySecPenguin	articles/CVE-2021-38001.md at main · vngkv123/articles github.com/vngkv123/artic…	2021-11-08 02:17:39
@0x0021h	github.com/vngkv123/artic…	2021-11-09 02:41:36
@CVEreport	CVE-2021-38001 : Type confusion in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potential… twitter.com/i/web/status/1…	2021-11-23 21:34:28
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution	2021-11-01 13:16:00

← Previous ID

Next ID→