



CVE-2021-38003

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

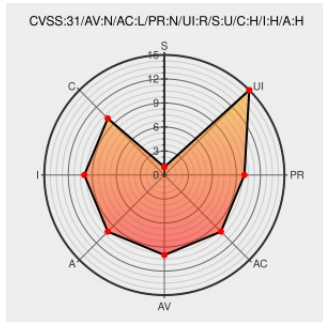
Last Modified on: 11/24/2021 04:21:00 PM UTC

CVE-2021-38003

Source: Mitre

Source: Nist

Print: PDF



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

Inappropriate implementation 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-2021-38003 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
1263462 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/1263462

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

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)
 @tukanana	“Googleは、CVE-2021-38000およびCVE-2021-38003の 익스プロイトが実際に存在することを認識しています。”0-day案件。 / 1件のコメント b.hatena.ne.jp/entry?url=http... “St... twitter.com/i/web/status/1...	2021-10-28 22:31:27
 @maddiestone	Two in-the-wild 0-days patched by Chrome: CVE-2021-38000 and CVE-2021-38003. Both discovered by Google TAG! @_clem1... twitter.com/i/web/status/1...	2021-10-28 23:50:08
 @ipssignatures	The vuln CVE-2021-38003 has a tweet created 0 days ago and retweeted 16 times. twitter.com/maddiestone/st... #pow1rtrtwcve	2021-10-29 02:06:01
 @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
 @okomeki	CVE-2021-38003はV8 JavaScriptの10代との高い不適切な実装バグ	2021-10-29 04:38:13
 @cKure7	████████ Zero-Day: Two in-the-wild 0-days patched by Chrome: CVE-2021-38000 and CVE-2021-38003. Both discovered by Goo... twitter.com/i/web/status/1...	2021-10-29 06:14:25
 @kr_simon_choi	Google is aware that exploits for CVE-2021-38000 and CVE-2021-38003 exist in the wild	2021-10-29 07:48:20
 @LaneSystems	#Google fixes two high-severity #ZeroDay flaws in #Chrome zdnet.com/article/google... CVE-2021-38000 & CVE-2021-38003.... twitter.com/i/web/status/1...	2021-10-29 11:10:11
 @AttackerKb	CVE-2021-38003, CVE-2021-38000, and CVE-2021-42258 have been reported as exploited in	2021-10-29

	the wild. attackerkb.com/activity-feed	14:26:50
 @z3r0trust	Consider updating Chrome today if you use it. "Google is aware that exploits for CVE-2021-38000 and CVE-2021-38003... twitter.com/i/web/status/1...	2021-10-29 15:34:38
 @appletester_rus	CVE-2021-38000 and CVE-2021-38003. The first of these, CVE-2021-38000, is described as "Insufficient verification o... twitter.com/i/web/status/1...	2021-10-29 18:22:20
 @appletester_rus	September 15, 2021. CVE-2021-38003 is an Inappropriate implementation bug in the Chrome V8 JavaScript engine. This... twitter.com/i/web/status/1...	2021-10-29 18:22:20
 @appletesterrus	CVE-2021-38000 and CVE-2021-38003. The first of these, CVE-2021-38000, is described as "Insufficient verification o... twitter.com/i/web/status/1...	2021-10-29 18:22:51
 @v_intestine	Edge の Stable 版で 95.0.1020.40 がリリースされました。 "This update contains a fix for CVE-2021-38000 and CVE-2021-38003 which... twitter.com/i/web/status/1...	2021-10-30 04:44:12
 @rkx73	#CVE-2021-38000 y #CVE-2021-38003 Dos vulnerabilidades día cero en #GoogleChrome noticiasseguridad.com/vulnerabilidad...	2021-10-30 06:48:37
 @management_sun	IT Risk: Microsoft.Edge (Chromium-based)に複数の脆弱性 -1/2 コード・コマンドを実行される サービス拒否に陥る セキュリティの低下 CVE-2021-38003 CVE-2021-380... twitter.com/i/web/status/1...	2021-11-01 13:08:04
 @linguini_elruso	RCE en chrome 95.0.4638.69 y anteriores CVE-2021-38000 CVE-2021-38003 Entre \$5k-\$25k, que la casería empiece ? Y... twitter.com/i/web/status/1...	2021-11-05 16:30:51
 @CVEreport	CVE-2021-38003 : Inappropriate implementation in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacke... twitter.com/i/web/status/1...	2021-11-23 21:35:03
 /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 →](#)

© CVE.report 2021   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report