



# CVE-2021-38002

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

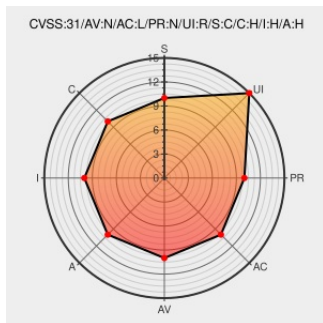
Last Modified on: 11/24/2021 04:27:00 PM UTC

## CVE-2021-38002

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



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

Use after free in Web Transport in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.

CVE-2021-38002 has been assigned by [chrome-cve-admin@google.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Google](#) - **Chrome** version < **95.0.4638.69**

CVSS3 Score: **9.6 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>PARTIAL</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
Chrome Releases: Stable Channel Update for Desktop	<a href="#">chromereleases.googleblog.com</a> <a href="#">text/html</a>	<a href="#">MISC</a> <a href="#">chromereleases.googleblog.com/2021/10/stable-</a>

1260940 - chromium - An open-source project to help move the web forward. - Monorail

crbug.com  
text/html

MISC crbug.com/1260940

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](mailto: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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-10-29 02:15:04
@CVEreport	CVE-2021-38002 : Use after free in Web Transport in Google Chrome prior to 95.0.4638.69 allowed a remote attacker t... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-11-23 21:34:40
/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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)