



CVE-2021-38005

Published on: 12/22/2021 12:00:00 AM UTC

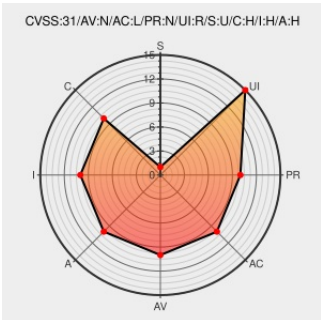
Last Modified on: 01/15/2022 03:15:00 PM UTC

CVE-2021-38005

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



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

Use after free in loader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-38005 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Google - Chrome** version < **96.0.4664.45**

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
Debian -- Security Information -- DSA-5046-1 chromium	www.debian.org Deprecated Link	DEBIAN DSA-5046

~~Deprecated Link~~
text/html

[SECURITY] Fedora 34 Update: chromium-96.0.4664.110-3.fc34 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2021-6a292e2cf4

Chrome Releases: Stable Channel Update for Desktop

chromereleases.googleblog.com
text/html

MISC
chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html

1241091 - chromium - An open-source project to help move the web forward. - Monorail

crbug.com
text/html

MISC crbug.com/1241091

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

[179000](#) Debian Security Update for chromium (DSA 5046-1)

[282220](#) Fedora Security Update for chromium (FEDORA-2021-6a292e2cf4)

[376055](#) Google Chrome Prior to 96.0.4664.45 Multiple Vulnerabilities

[376092](#) Microsoft Edge Based on Chromium Prior to 96.0.1054.29 Multiple Vulnerabilities

[690240](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (b8c0cbca-472d-11ec-83dc-3065ec8fd3ec)

[751564](#) OpenSUSE Security Update for chromium (openSUSE-SU-2021:1632-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All
<pre>cpe:2.3:a:google:chrome:.*:.*:.*:.*:.*:.*</pre>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEannounce	CVE-2021-38008, CVE-2021-38009, CVE-2021-38006, CVE-2021-38005, CVE-2021-38010, CVE-2021-38011 forbes.com/sites/gordonke...	2021-11-18 15:12:53
@vigilance_fr	Vigil@nce #Vulnérabilité de Chrome : multiples vulnérabilités. vigilance.fr/vulnerabilite/... Références : #CVE-2021-38005... twitter.com/i/web/status/1...	2021-11-22 12:09:03
@vigilance_en	Vigil@nce #Vulnerability of Chrome: multiple vulnerabilities. vigilance.fr/vulnerability/... Identifiers: #CVE-2021-38005,... twitter.com/i/web/status/1...	2021-11-22 12:09:04
@CVEreport	CVE-2021-38005 : Use after free in loader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to poten... twitter.com/i/web/status/1...	2021-12-23 00:09:24
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution	2021-11-16 14:20:54

© CVE.report 2022 [🐦](#) [N](#) |

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](#)