



CVE-2022-3655

Published on: Not Yet Published

Last Modified on: 12/09/2022 03:46:00 PM UTC

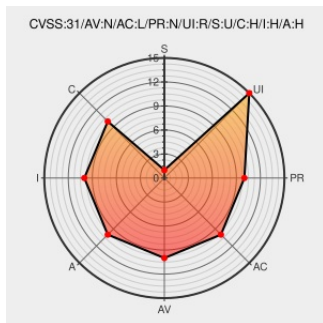
CVE-2022-3655

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Heap buffer overflow in Media Galleries in Google Chrome prior to 107.0.5304.62 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)

CVE-2022-3655 has been assigned by [chrome-cve-admin@google.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Google](#) - **Chrome** version < 107.0.5304.62

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

CVE References

Description	Tags	Link
Chrome Releases: Stable Channel Update for Desktop	chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html
1343384 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/1343384

By selecting these links, you may be leaving CVEreport workspace. 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

[181168](#) Debian Security Update for chromium (DSA 5261-1)

[182868](#) Debian Security Update for chromium (CVE-2022-3655)

[377698](#) Google Chrome Prior to 107.0.5304.62 Multiple Vulnerabilities

[377720](#) Microsoft Edge Based on Chromium Prior to 107.0.1418.24 Multiple Vulnerabilities

[690969](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (b4ef02f4-549f-11ed-8ad9-3065ec8fd3ec)

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)
 @vuldb	[Vuln] A new vulnerability with increased severity was disclosed for Google Chrome (CVE-2022-3655) vuldb.com/?id.212312	2022-10-26 18:11:03
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY – Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution – PATCH: NOW	2022-10-26 13:00:35
 /r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY – Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution – PATCH: NOW	2022-10-31 21:27:22
 /r/netcve	CVE-2022-3655	2022-11-02 00:38:44

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)