



CVE-2022-2620

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

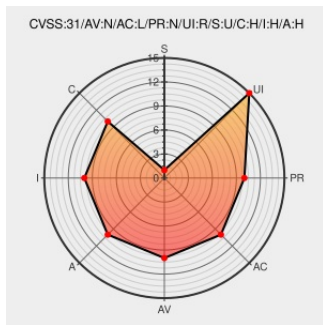
CVE-2022-2620

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Fedora** from **Fedoraproject** contain the following vulnerability:

Use after free in WebUI in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.

CVE-2022-2620 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Google - Chrome** version < **104.0.5112.79**

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
1337304 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/1337304
[SECURITY] Fedora 37 Update: chromium-105.0.5195.125-2.fc37 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-3f28aa88cf
Chrome Releases: Stable Channel Update for Desktop	chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html
Chromium, Google Chrome, Microsoft Edge: Multiple Vulnerabilities (GLSA 202208-35) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202208-35

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

[180919](#) Debian Security Update for chromium (DSA 5201-1)

[184737](#) Debian Security Update for chromium (CVE-2022-2620)

[283172](#) Fedora Security Update for chromium (FEDORA-2022-3ca063941b)

[283173](#) Fedora Security Update for chromium (FEDORA-2022-b49c9bc07a)

[376772](#) Google Chrome Prior to 104.0.5112.79 Multiple Vulnerabilities

[690907](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (96a41723-133a-11ed-be3b-3065ec8fd3ec)





[710606](#) Gentoo Linux Chromium, Google Chrome, Microsoft Edge Multiple Vulnerabilities (GLSA 202208-35)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
<code>cpe:2.3:o:fedoraproject:fedora:37:*:*:*:*:*:</code>						
<code>cpe:2.3:a:google:chrome:*:*:*:*:*:</code>						
<code>cpe:2.3:o:google:chrome_os:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-2620 : Use after free in WebUI in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attac... twitter.com/i/web/status/1...	2022-08-12 19:51:39
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-2620 Use after free in WebUI in Google Chrome on Chrome OS prior to 104... twitter.com/i/web/status/1...	2022-08-12 21:56:01
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-08-03 21:06:30
 /r/netcve	CVE-2022-2620	2022-08-12 20:38:40

[← 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](#)