



# CVE-2021-21228

Published on: 04/30/2021 12:00:00 AM UTC

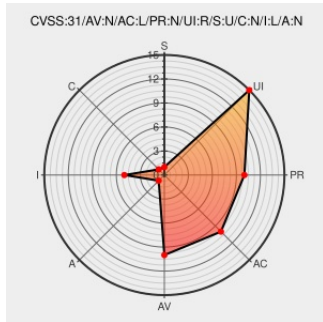
Last Modified on: 06/01/2021 02:42:00 PM UTC

## CVE-2021-21228

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Insufficient policy enforcement in extensions in Google Chrome prior to 90.0.4430.93 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.

CVE-2021-21228 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Google - Chrome** version < **90.0.4430.93**

CVSS3 Score: **4.3 - MEDIUM**

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>UNCHANGED</b>	<b>NONE</b>	<b>LOW</b>	<b>NONE</b>

CVSS2 Score: **4.3 - MEDIUM**

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

## CVE References

Description	Tags	Link
Chromium, Google Chrome: Multiple vulnerabilities (GI SA 202104-08) — Gentoo security	<a href="#">security.gentoo.org</a> <a href="#">text/html</a>	<a href="#">GENTOO GLSA-202104-08</a>

Chrome Releases: Stable Channel Update for Desktop	<a href="https://chromereleases.googleblog.com">chromereleases.googleblog.com</a> text/html	MISC <a href="https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html">chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html</a>
[SECURITY] Fedora 33 Update: chromium-90.0.4430.93-1.fc33 - package-announce - Fedora Mailing-Lists	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> text/html	FEDORA FEDORA-2021-35d2bb4627
[SECURITY] Fedora 34 Update: chromium-90.0.4430.93-1.fc34 - package-announce - Fedora Mailing-Lists	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> text/html	FEDORA FEDORA-2021-c3754414e7
1139156 - chromium - An open-source project to help move the web forward. - Monorail	<a href="https://crbug.com">crbug.com</a> text/html	MISC <a href="https://crbug.com/1139156">crbug.com/1139156</a>
[SECURITY] Fedora 32 Update: chromium-90.0.4430.93-1.fc32 - package-announce - Fedora Mailing-Lists	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> text/html	FEDORA FEDORA-2021-ff893e12c5
Debian -- Security Information -- DSA-4911-1 chromium	<a href="https://www.debian.org">www.debian.org</a> <b>Deprecated Link</b> text/html	DEBIAN DSA-4911

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

- [178575](#) Debian Security Update for chromium (DSA 4911-1)
- [281203](#) Fedora Security Update for chromium (FEDORA-2021-35d2bb4627)
- [281204](#) Fedora Security Update for chromium (FEDORA-2021-ff893e12c5)
- [281205](#) Fedora Security Update for chromium (FEDORA-2021-c3754414e7)
- [375505](#) Google Chrome Prior To 90.0.4430.93 Multiple Vulnerabilities
- [375526](#) Microsoft Edge Based On Chromium Prior to 90.0.818.51 Multiple Vulnerabilities
- [710018](#) Gentoo Linux Chromium, Google Chrome Multiple Vulnerabilities (GLSA 202104-08)

## Known Affected Configurations (CPE V2.3)



Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All

...cpe:2.3-o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*

cpe:2.3:o:debian:debian_linux:10.0:*****:
cpe:2.3:o:fedoraproject:fedora:32:*****:
cpe:2.3:o:fedoraproject:fedora:33:*****:
cpe:2.3:o:fedoraproject:fedora:34:*****:
cpe:2.3:a:google:chrome:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2021-21228 : Insufficient policy enforcement in extensions in Google Chrome prior to 90.0.4430.93 allowed an at... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-04-30 20:19:09
 /r/netcve	<a href="#">CVE-2021-21228</a>	2021-04-30 20:41:56

[← 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](https://status.cve.report)**