



# CVE-2021-30518

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-30518
<b>State</b>	PUBLIC
<b>Assigner</b>	chrome-cve-admin@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-04 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:33:00 UTC
<b>Description</b>	Heap buffer overflow in Reader Mode in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

## References

Reference	Source	Link
[SECURITY] Fedora 34 Update: chromium-91.0.4472.114-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Chrome Releases: Stable Channel Update for Desktop	MISC	<a href="#">chromereleases.googleblog.com</a>
1203590 - chromium - An open-source project to help move the web forward. - Monorail	MISC	<a href="#">crbug.com</a>
[SECURITY] Fedora 34 Update: chromium-91.0.4472.114-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: chromium-91.0.4472.114-2.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: chromium-91.0.4472.114-2.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202107-06) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

178603 Debian Security Update for chromium (DSA 4917-1)

179531 Debian Security Update for chromium (CVE-2021-30518)

281103 Fedora Security Update for chromium (FEDORA-2021-54683b0888)

281104 Fedora Security Update for chromium (FEDORA-2021-7190a83164)

281696 Fedora Security Update for chromium (FEDORA-2021-f94dadff78)

281724 Fedora Security Update for chromium (FEDORA-2021-ca58c57bdf)

375546 Google Chrome Prior To 90.0.4430.212 Multiple Vulnerabilities

375575 Microsoft Edge Based On Chromium Prior to 90.0.818.62 Multiple Vulnerabilities

501912 Alpine Linux Security Update for qt5-qtwebengine

690142 Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (3cac007f-b27e-11eb-97a0-e09467587c17)

710070 Gentoo Linux Chromium, Google Chrome Multiple vulnerabilities (GLSA 202107-06)

750178 OpenSUSE Security Update for opera (openSUSE-SU-2021:0829-1)

750179 OpenSUSE Security Update for opera (openSUSE-SU-2021:0828-1)

750203 OpenSUSE Security Update for chromium (openSUSE-SU-2021:0762-1)

750209 OpenSUSE Security Update for chromium (openSUSE-SU-2021:0742-1)

751978 OpenSUSE Security Update for opera (openSUSE-SU-2022:0110-1)

© [CVE.report](#) 2026 |

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](#)