



# CVE-2021-21148

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

## Summary

<b>CVE</b>	CVE-2021-21148
<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>	2021-02-09 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:29:00 UTC
<b>Description</b>	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.150 allowed a remote attacker to potentially exploit heap c

## Risk And Classification

**EPSS:** 0.248710000 probability, percentile 0.961190000 (date 2026-04-01)

**CISA KEV:** Listed on 2021-11-03; due 2021-11-17; ransomware use Unknown

**Problem Types:** CWE-787

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Google
<b>Product</b>	Chromium V8
<b>Name</b>	Google Chromium V8 Heap Buffer Overflow Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-21148">https://nvd.nist.gov/vuln/detail/CVE-2021-21148</a>

## NVD Known Affected Configurations (CPE 2.3)

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="#">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>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All

## References

Reference	Source	Link
Chrome Array Transfer Bypass ≈ Packet Storm	MISC	<a href="#">packetstormsecu</a>
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202104-08) — Gentoo security	GENTOO	<a href="#">security.gentoo.o</a>
Chrome Releases: Stable Channel Update for Desktop	MISC	<a href="#">chromereleases.c</a>
1170176 - chromium - An open-source project to help move the web forward. - Monorail	MISC	<a href="#">crbug.com</a>
[SECURITY] Fedora 33 Update: chromium-88.0.4324.150-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject</a>
[SECURITY] Fedora 32 Update: chromium-88.0.4324.150-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject</a>
[SECURITY] Fedora 33 Update: chromium-88.0.4324.150-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject</a>
[SECURITY] Fedora 32 Update: chromium-88.0.4324.150-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject</a>
Debian -- Security Information -- DSA-4858-1 chromium	DEBIAN	<a href="#">www.debian.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="#">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- [180427](#) Debian Security Update for chromium (CVE-2021-21148)
- [501447](#) Alpine Linux Security Update for nodejs
- [501910](#) Alpine Linux Security Update for qt5-qtwebengine
- [504203](#) Alpine Linux Security Update for nodejs
- [505349](#) Alpine Linux Security Update for qt5-qtwebengine
- [690363](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (3e01aad2-680e-11eb-83e2-e09467587c17)
- [710018](#) Gentoo Linux Chromium, Google Chrome Multiple Vulnerabilities (GLSA 202104-08)
- [750316](#) OpenSUSE Security Update for opera (openSUSE-SU-2021:0413-1)
- [750359](#) OpenSUSE Security Update for opera (openSUSE-SU-2021:0296-1)
- [750368](#) OpenSUSE Security Update for chromium (openSUSE-SU-2021:0267-1)
- [750825](#) OpenSUSE Security Update for libqt5-qtwebengine (openSUSE-SU-2021:0973-1)

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](#)**