



CVE-2021-21157

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-21157 |
| State | PUBLIC |
| Assigner | chrome-cve-admin@google.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-02-22 22:15:00 UTC |
| Updated | 2023-11-07 03:29:00 UTC |
| Description | Use after free in Web Sockets in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially e: |

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|-------------------------------|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Application | Google | Chrome | All | All | All | All |
| Application | Google | Chrome | All | All | All | All |
| Operating System | Linux | Linux Kernel | - | All | All | All |
| Operating System | Linux | Linux Kernel | - | All | All | All |
| Operating System | Linux | Linux Kernel | - | All | All | All |
| Application | Microsoft | Edge | All | All | All | All |
| Application | Microsoft | Edge | All | All | All | All |
| Application | Microsoft | Edge Chromium | All | All | All | All |
| Application | Microsoft | Edge Chromium | All | All | All | All |

References

| Reference | Source | Link |
|--|--------|-------------------------------------|
| [SECURITY] Fedora 33 Update: chromium-88.0.4324.182-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| [SECURITY] Fedora 32 Update: chromium-89.0.4389.82-1.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |

| | | |
|--|---------|---|
| Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202104-08) — Gentoo security | GENTOO | security.gentoo.o |
| 1170657 - chromium - An open-source project to help move the web forward. - Monorail | MISC | crbug.com |
| Chrome Releases: Stable Channel Update for Desktop | MISC | chromereleases.g |
| [SECURITY] Fedora 33 Update: chromium-88.0.4324.182-1.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |
| [SECURITY] Fedora 32 Update: chromium-89.0.4389.82-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 180064 Debian Security Update for chromium (CVE-2021-21157) |
| 281482 Fedora Security Update for chromium (FEDORA-2021-c88a96bd4b) |
| 501910 Alpine Linux Security Update for qt5-qtwebengine |
| 505349 Alpine Linux Security Update for qt5-qtwebengine |
| 690381 Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (48514901-711d-11eb-9846-e09467587c17) |
| 710018 Gentoo Linux Chromium, Google Chrome Multiple Vulnerabilities (GLSA 202104-08) |
| 750316 OpenSUSE Security Update for opera (openSUSE-SU-2021:0413-1) |
| 750325 OpenSUSE Security Update for chromium (openSUSE-SU-2021:0392-1) |
| 750825 OpenSUSE Security Update for libqt5-qtwebengine (openSUSE-SU-2021:0973-1) |

© [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](#)