



# CVE-2021-28116

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-28116  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2021-03-09 22:15:00 UTC   |
| <b>Updated</b>         | 2023-11-07 03:32:00 UTC   |
| <b>Description</b>     | Squid through 4.14 and 5.x through 5.0.5, in some configurations, allows information disclosure because of an out-of-bounds |

## Risk And Classification

**Problem Types:** CWE-125

## 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> | 11.0    | 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="#">Squid-cache</a>   | <a href="#">Squid</a>        | All     | All    | All     | All      |
| Application      | <a href="#">Squid-cache</a>   | <a href="#">Squid</a>        | All     | All    | All     | All      |

## References

| Reference   | Source | Link   |
|---|--------|--|
| oss-security - CVE-2021-28116 / ZDI-CAN-11610 / SQUID-2020:12 Out-Of-Bounds memory access in WCCPv2 | MLIST  | <a href="http://www.openwall.com/lists/oss-security">www.openwall.com/lists/oss-security</a> |
| [SECURITY] Fedora 33 Update: squid-4.15-1.fc33 - package-announce - Fedora Mailing-Lists            | FEDORA | <a href="mailto:lists.fedoraproject.org">lists.fedoraproject.org</a>                         |
| Debian -- Security Information -- DSA-5171-1 squid  | DEBIAN | <a href="http://www.debian.org/security">www.debian.org/security</a>                         |
| [SECURITY] Fedora 33 Update: squid-4.15-1.fc33 - package-announce - Fedora Mailing-Lists            |        | <a href="mailto:lists.fedoraproject.org">lists.fedoraproject.org</a>                         |
| ZDI-21-157   Zero Day Initiative  | MISC   | <a href="http://www.zerodayinitiative.com">www.zerodayinitiative.com</a>                     |
| squid : Optimising Web Delivery   | MISC   | <a href="http://www.squid-cache.org">www.squid-cache.org</a>                                 |
| Squid: Multiple vulnerabilities (GLSA 202105-14) — Gentoo security                                  | GENTOO | <a href="http://security.gentoo.org">security.gentoo.org</a>                                 |
| [SECURITY] Fedora 34 Update: squid-5.0.6-1.fc34 - package-announce - Fedora Mailing-Lists           | FEDORA | <a href="mailto:lists.fedoraproject.org">lists.fedoraproject.org</a>                         |

[github.com/squid-cache/squid/security/advisories/GHSA-rgf3-9v3p-qp82](https://github.com/squid-cache/squid/security/advisories/GHSA-rgf3-9v3p-qp82)

MISC

[github.com](https://github.com)

CVE Program record

CVE.ORG

[www.cve.org](https://www.cve.org)

NVD vulnerability detail

NVD

[nvd.nist.gov](https://nvd.nist.gov)

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159831](#) Oracle Enterprise Linux Security Update for squid:4 (ELSA-2022-1939)

[179566](#) Debian Security Update for squid (DSA 5171-1)

[183930](#) Debian Security Update for squid (CVE-2021-28116)

[198532](#) Ubuntu Security Notification for Squid Vulnerability (USN-5104-1)

[240284](#) Red Hat Update for squid:4 (RHSA-2022:1939)

[281619](#) Fedora Security Update for squid (FEDORA-2021-c0bec55ec7)

[281620](#) Fedora Security Update for squid (FEDORA-2021-24af72ff2c)

[296065](#) Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)

[356184](#) Amazon Linux Security Advisory for squid : ALASSQUID4-2023-004

[356430](#) Amazon Linux Security Advisory for squid : ALAS2-2023-2318

[500662](#) Alpine Linux Security Update for squid

[501498](#) Alpine Linux Security Update for squid

[502033](#) Alpine Linux Security Update for squid

[504434](#) Alpine Linux Security Update for squid

[671160](#) EulerOS Security Update for squid (EulerOS-SA-2021-2815)

[671714](#) EulerOS Security Update for squid (EulerOS-SA-2022-1766)

[671830](#) EulerOS Security Update for squid (EulerOS-SA-2022-1916)

[710101](#) Gentoo Linux Squid Multiple vulnerabilities (GLSA 202105-14)

[751209](#) SUSE Enterprise Linux Security Update for squid (SUSE-SU-2021:3334-1)

[751267](#) OpenSUSE Security Update for squid (openSUSE-SU-2021:3485-1)

[751309](#) OpenSUSE Security Update for squid (openSUSE-SU-2021:1419-1)

[940533](#) AlmaLinux Security Update for squid:4 (ALSA-2022:1939)

© [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](#)**