



# CVE-2024-23638

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2024-23638                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Unknown                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2024-01-24 00:15:00 UTC                      |
| <b>Updated</b>         | 2024-01-30 23:05:00 UTC                      |
| <b>Description</b>     | Description unavailable.                     |

## Risk And Classification

**Problem Types:** CWE-672

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                      | Product               | Version | Update | Edition | Language |
|-------------|-----------------------------|-----------------------|---------|--------|---------|----------|
| 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                                 | Tags |
|---|---------|--------------------------------------|------|
| Just close after a write(2) response sending error (#1582) · squid-cache/squid@290ae20 · GitHub |         | <a href="#">github.com</a>           | Pe   |
| <a href="#">www.squid-cache.org/Versions/v5/SQUID-2023_11.patch</a>                             |         | <a href="#">www.squid-cache.org</a>  | M    |
| <a href="#">www.squid-cache.org/Versions/v6/SQUID-2023_11.patch</a>                             |         | <a href="#">www.squid-cache.org</a>  | M    |
| 6.6 (#1615) · squid-cache/squid@e8118a7 · GitHub  |         | <a href="#">github.com</a>           | Pe   |
| Implicit Assertion in Stream Handling   Squid-Security-Audit                                    |         | <a href="#">megamansec.github.io</a> | Ex   |
| SQUID-2023:11 Denial of Service in Cache Manager · Advisory · squid-cache/squid · GitHub        |         | <a href="#">github.com</a>           | Ve   |
| CVE Program record  | CVE.ORG | <a href="#">www.cve.org</a>          | ca   |
| NVD vulnerability detail  | NVD     | <a href="#">nvd.nist.gov</a>         | ca   |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

|  |
|--|
| <a href="#">200247</a> Ubuntu Security Notification for Squid Vulnerabilities (USN-6728-1)   |
| <a href="#">357076</a> Amazon Linux Security Advisory for squid : ALAS2-2024-2433            |
| <a href="#">357373</a> Amazon Linux Security Advisory for squid : ALAS2023-2024-578          |
| <a href="#">379320</a> Squid Proxy Denial of Service (DoS) Vulnerability (SQUID-2023:11)     |
| <a href="#">6000513</a> Debian Security Update for squid (DSA 5637-1)                        |
| <a href="#">755686</a> SUSE Enterprise Linux Security Update for squid (SUSE-SU-2024:0296-1) |
| <a href="#">755690</a> SUSE Enterprise Linux Security Update for squid (SUSE-SU-2024:0298-1) |
| <a href="#">755742</a> SUSE Enterprise Linux Security Update for squid (SUSE-SU-2024:0455-1) |

© [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](#)**