



# CVE-2022-41317

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

## Summary

<b>CVE</b>	CVE-2022-41317
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-25 19:15:00 UTC
<b>Updated</b>	2023-08-08 14:22:00 UTC
<b>Description</b>	An issue was discovered in Squid 4.9 through 4.17 and 5.0.6 through 5.6. Due to inconsistent handling of internal URIs, the

## Risk And Classification

**Problem Types:** CWE-697

## 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
<a href="http://www.squid-cache.org/Versions/v5/changesets/SQUID-2022_1.patch">www.squid-cache.org/Versions/v5/changesets/SQUID-2022_1.patch</a>	MISC	<a href="http://www.squid-cache.org">www.squid-cache.org</a>
<a href="#">oss-security - Fwd: [ADVISORY] SQUID-2022:1 Exposure of Sensitive Information in Cache Manager</a>	CONFIRM	<a href="http://www.openwall.com">www.openwall.com</a>
<a href="http://www.squid-cache.org/Versions/v4/changesets/SQUID-2022_1.patch">www.squid-cache.org/Versions/v4/changesets/SQUID-2022_1.patch</a>	MISC	<a href="http://www.squid-cache.org">www.squid-cache.org</a>
<a href="#">SQUID-2022:1 Exposure of Sensitive Information in Cache Manager · Advisory · squid-cache/squid · GitHub</a>	MISC	<a href="https://github.com">github.com</a>
<a href="#">CVE Program record</a>	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
<a href="#">NVD vulnerability detail</a>	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[181132](#) Debian Security Update for squid (DLA 3151-1)

[181146](#) Debian Security Update for squid (DSA 5258-1)

184816 Debian Security Update for squid (CVE-2022-41317)
198961 Ubuntu Security Notification for Squid Vulnerabilities (USN-5641-1)
283170 Fedora Security Update for squid (FEDORA-2022-c8cad41c95)
283171 Fedora Security Update for squid (FEDORA-2022-23e6ee1fb9)
354752 Amazon Linux Security Advisory for squid : ALAS-2023-1687
354783 Amazon Linux Security Advisory for squid : ALAS2-2023-1950
356199 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-009
356205 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-002
356506 Amazon Linux Security Advisory for squid : ALAS2SQUID4-2023-002
356609 Amazon Linux Security Advisory for squid : ALAS2SQUID4-2023-010
505939 Alpine Linux Security Update for squid
672417 EulerOS Security Update for squid (EulerOS-SA-2022-2807)
690944 Free Berkeley Software Distribution (FreeBSD) Security Update for squid (f9ada0b5-3d80-11ed-9330-080027f5fec9)
752660 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2022:3533-1)
752662 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2022:3532-1)
752677 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2022:3596-1)
753450 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2022:3531-1)

© [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](#)**