



CVE-2022-41318

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-41318
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-25 19:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	A buffer over-read was discovered in libntlmauth in Squid 2.5 through 5.6. Due to incorrect integer-overflow protection, the s

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squid-cache	Squid	All	All	All	All

References

Reference	Source	Link
www.squid-cache.org/Versions/v5/changesets/SQUID-2022_2_patch	MISC	www.squid-cache.org
SQUID-2022:2 Buffer Over Read in SSPI and SMB Authentication · Advisory · squid-cache/squid · GitHub	MISC	github.com
oss-security - Fwd: [ADVISORY] SQUID-2022:2 Buffer Over Read in SSPI and SMB Authentication	CONFIRM	www.openwall.com
www.squid-cache.org/Versions/v4/changesets/SQUID-2022_2_patch	MISC	www.squid-cache.org
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

160124 Oracle Enterprise Linux Security Update for squid:4 (ELSA-2022-6775)

160129 Oracle Enterprise Linux Security Update for squid (ELSA-2022-6815)

160130 Oracle Enterprise Linux Security Update for squid (ELSA-2022-6820)

160130 Oracle Enterprise Linux Security Update for squid (ELSA-2022-6839)
181132 Debian Security Update for squid (DLA 3151-1)
181146 Debian Security Update for squid (DSA 5258-1)
183242 Debian Security Update for squid (CVE-2022-41318)
198961 Ubuntu Security Notification for Squid Vulnerabilities (USN-5641-1)
240704 Red Hat Update for squid:4 (RHSA-2022:6775)
240705 Red Hat Update for squid:4 (RHSA-2022:6776)
240709 Red Hat Update for squid:4 (RHSA-2022:6777)
240710 Red Hat Update for squid (RHSA-2022:6815)
240719 Red Hat Update for squid (RHSA-2022:6839)
257196 CentOS Security Update for squid (CESA-2022:6815)
283170 Fedora Security Update for squid (FEDORA-2022-c8cad41c95)
283171 Fedora Security Update for squid (FEDORA-2022-23e6ee1fb9)
354655 Amazon Linux Security Advisory for squid : ALAS2-2023-1907
354715 Amazon Linux Security Advisory for squid : ALAS-2023-1677
355074 Amazon Linux Security Advisory for squid : AL2012-2023-398
356225 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-001
377620 Alibaba Cloud Linux Security Update for squid (ALINUX2-SA-2022:0042)
377623 Alibaba Cloud Linux Security Update for squid:4 (ALINUX3-SA-2022:0166)
503692 Alpine Linux Security Update for squid
672417 EulerOS Security Update for squid (EulerOS-SA-2022-2807)
672715 EulerOS Security Update for squid (EulerOS-SA-2023-1515)
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)
940660 AlmaLinux Security Update for squid (ALSA-2022:6839)
940677 AlmaLinux Security Update for squid:4 (ALSA-2022:6775)
960289 Rocky Linux Security Update for squid:4 (RLSA-2022:6775)

© [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](#)