



CVE-2019-12520

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

Summary

CVE	CVE-2019-12520
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-15 20:15:00 UTC
Updated	2021-02-11 14:42:00 UTC
Description	An issue was discovered in Squid through 4.7 and 5. When receiving a request, Squid checks its cache to see if it can serv

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Squid-cache	Squid	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 2278-1] squid3 security update	MLIST	lists.debian.org	Mailing List, Third P
January 2021 Squid Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Third Party Advisory
squid : Optimising Web Delivery	MISC	www.squid-cache.org	Release Notes, Ven
Squid 4 changes	MISC	www.squid-cache.org	Release Notes, Ven
USN-4446-1: Squid vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Advisory

Debian -- Security Information -- DSA-4682-1 squid	DEBIAN	www.debian.org	Third Party Advisory
squid/CVEs/CVE-2019-12520.txt · master · Jeriko One / Security · GitLab	MISC	gitlab.com	Third Party Advisory
Commits · squid-cache/squid · GitHub	MISC	github.com	Patch, Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159658 Oracle Enterprise Linux Security Update for squid:4 (ELSA-2020-4743)
160118 Oracle Enterprise Linux Security Update for squid (ELSA-2022-22254)
356199 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-009
356609 Amazon Linux Security Advisory for squid : ALAS2SQUID4-2023-010
377360 Alibaba Cloud Linux Security Update for squid:4 (ALINUX3-SA-2022:0124)
671714 EulerOS Security Update for squid (EulerOS-SA-2022-1766)
940034 AlmaLinux Security Update for squid:4 (ALSA-2020:4743)
960867 Rocky Linux Security Update for squid:4 (RLSA-2020:4743)

© [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](#)