



CVE-2019-12521

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-12521 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-04-15 19:15:00 UTC |
| Updated | 2021-07-21 11:39:00 UTC |
| Description | An issue was discovered in Squid through 4.7. When Squid is parsing ESI, it keeps the ESI elements in ESIContext. ESICo |

Risk And Classification

Problem Types: CWE-787 | CWE-193

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 | 19.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 20.04 | 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 | Canonical | Ubuntu Linux | 19.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 20.04 | 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 |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Squid-cache | Squid | All | All | All | All |
| Application | Squid-cache | Squid | All | 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, Tr |
| January 2021 Squid Vulnerabilities in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | Third Party Ad |
| squid/CVEs/CVE-2019-12521.txt · master · Jeriko One / Security · GitLab | MISC | gitlab.com | Third Party Ad |
| [security-announce] openSUSE-SU-2020:0623-1: important: Security update | SUSE | lists.opensuse.org | Mailing List, Tr |
| Squid: Multiple vulnerabilities (GLSA 202005-05) — Gentoo security | GENTOO | security.gentoo.org | Third Party Ad |
| Debian -- Security Information -- DSA-4682-1 squid | DEBIAN | www.debian.org | Third Party Ad |
| USN-4356-1: Squid vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | usn.ubuntu.com | Third Party Ad |
| oss-security - [ADVISORY] SQUID-2019:12 Multiple issues in ESI Response processing | MLIST | www.openwall.com | Mailing List, Pa |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, ana |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159658](#) Oracle Enterprise Linux Security Update for squid:4 (ELSA-2020-4743)
- [296074](#) Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)
- [356292](#) Amazon Linux Security Advisory for squid : ALASSQUID4-2023-008
- [357357](#) Amazon Linux Security Advisory for squid : ALAS2-2024-2509
- [377360](#) Alibaba Cloud Linux Security Update for squid:4 (ALINUX3-SA-2022:0124)
- [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