



CVE-2020-25097

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-25097 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-03-19 05:15:00 UTC |
| Updated | 2023-11-07 03:20:00 UTC |
| Description | An issue was discovered in Squid through 4.13 and 5.x through 5.0.4. Due to improper input validation, it allows a trusted cl |

Risk And Classification

Problem Types: CWE-20 | CWE-444

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|-------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Application | Netapp | Cloud Manager | - | All | All | All |
| Application | Squid-cache | Squid | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|--------|---|------|
| [SECURITY] Fedora 32 Update: squid-4.14-1.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| www.squid-cache.org/Versions/v5/changesets/SQUID-2020_11.patch | MISC | www.squid-cache.org | |
| www.squid-cache.org/Versions/v4/changesets/SQUID-2020_11.patch | MISC | www.squid-cache.org | |
| SQUID-2020:11 HTTP Request Smuggling · Advisory · squid-cache/squid · GitHub | MISC | github.com | |
| [SECURITY] Fedora 34 Update: squid-4.14-1.fc34 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| [SECURITY] Fedora 34 Update: squid-4.14-1.fc34 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org | |
| [SECURITY] Fedora 33 Update: squid-4.14-1.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| [SECURITY] Fedora 32 Update: squid-4.14-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org | |

| | | | |
|--|---------|---|-------------|
| CVE-2020-25097 Squid Vulnerability in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | |
| [SECURITY] Fedora 33 Update: squid-4.14-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org | |
| Debian -- Security Information -- DSA-4873-1 squid | DEBIAN | www.debian.org | Third Party |
| Squid: Multiple vulnerabilities (GLSA 202105-14) — Gentoo security | GENTOO | security.gentoo.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 159145 Oracle Enterprise Linux Security Update for squid (ELSA-2021-1135) |
| 159230 Oracle Enterprise Linux Security Update for squid:4 (ELSA-2021-1979) |
| 178496 Debian Security Update for squid3 (DLA 2598-1) |
| 178520 Debian Security Update for squid (DSA 4873-1) |
| 198313 Ubuntu Security Notification for Squid, Squid3 Vulnerabilities (USN-4895-1) |
| 239216 Red Hat Update for squid (RHSA-2021:1135) |
| 239282 Red Hat Update for squid:4 (RHSA-2021:2025) |
| 239286 Red Hat Update for squid:4 (RHSA-2021:1979) |
| 257077 CentOS Security Update for squid (CESA-2021:1135) |
| 281387 Fedora Security Update for squid (FEDORA-2021-7d86bec29e) |
| 281388 Fedora Security Update for squid (FEDORA-2021-ecb24e0b9d) |
| 281389 Fedora Security Update for squid (FEDORA-2021-76f09062a7) |
| 296065 Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021) |
| 352267 Amazon Linux Security Advisory for squid: ALAS2-2021-1631 |
| 352273 Amazon Linux Security Advisory for squid: ALAS2-2021-1631 |
| 356290 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-005 |
| 375397 Squid HTTP Request Smuggling Vulnerability (SQUID-2020:11) |
| 377074 Alibaba Cloud Linux Security Update for squid (ALINUX2-SA-2021:0019) |
| 500660 Alpine Linux Security Update for squid |
| 501496 Alpine Linux Security Update for squid |

| |
|--|
| 504432 Alpine Linux Security Update for squid |
| 670223 EulerOS Security Update for squid (EulerOS-SA-2021-1852) |
| 670410 EulerOS Security Update for squid (EulerOS-SA-2021-1989) |
| 670473 EulerOS Security Update for squid (EulerOS-SA-2021-2231) |
| 670675 EulerOS Security Update for squid (EulerOS-SA-2021-2433) |
| 670916 EulerOS Security Update for squid (EulerOS-SA-2021-2433) |
| 710101 Gentoo Linux Squid Multiple vulnerabilities (GLSA 202105-14) |
| 750098 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2021:1838-1) |
| 750160 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2021:1961-1) |
| 750641 OpenSUSE Security Update for squid (openSUSE-SU-2021:0879-1) |
| 750782 OpenSUSE Security Update for squid (openSUSE-SU-2021:1961-1) |
| 752348 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2022:2392-1) |
| 753288 SUSE Enterprise Linux Security Update for squid3 (SUSE-SU-2022:14914-1) |
| 940351 AlmaLinux Security Update for squid:4 (ALSA-2021:1979) |
| 960012 Rocky Linux Security Update for squid:4 (RLSA-2021:1979) |

© [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](#)