



# CVE-2020-15810

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

## Summary

|                        |                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2020-15810                                                                                                          |
| <b>State</b>           | PUBLIC                                                                                                                  |
| <b>Assigner</b>        | cve@mitre.org                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                            |
| <b>Published</b>       | 2020-09-02 17:15:00 UTC                                                                                                 |
| <b>Updated</b>         | 2023-11-07 03:17:00 UTC                                                                                                 |
| <b>Description</b>     | An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Smugg |

## Risk And Classification

**Problem Types:** CWE-444

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                      | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 18.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 20.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 18.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 20.04   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 31      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 32      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 33      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 31      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 32      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 33      | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>      | <a href="#">Leap</a>         | 15.1    | All    | All     | All      |

|                  |                             |                       |      |     |     |     |
|------------------|-----------------------------|-----------------------|------|-----|-----|-----|
| Operating System | <a href="#">Opensuse</a>    | <a href="#">Leap</a>  | 15.2 | All | All | All |
| Operating System | <a href="#">Opensuse</a>    | <a href="#">Leap</a>  | 15.1 | All | All | All |
| Operating System | <a href="#">Opensuse</a>    | <a href="#">Leap</a>  | 15.2 | All | All | All |
| 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                                                                  | Tags     |
|------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------------|----------|
| NetApp Product Security                                                                  | CONFIRM | <a href="https://security.netapp.com">security.netapp.com</a>         | Broken   |
| SQUID-2020:10 HTTP(S) Request Smuggling · Advisory · squid-cache/squid · GitHub          | MISC    | <a href="https://github.com">github.com</a>                           | Mitigati |
| [SECURITY] Fedora 31 Update: squid-4.13-1.fc31 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Third Pa |
| Debian -- Security Information -- DSA-4751-1 squid                                       | DEBIAN  | <a href="https://www.debian.org">www.debian.org</a>                   | Third Pa |
| [SECURITY] Fedora 33 Update: squid-4.13-1.fc33 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |          |
| [SECURITY] Fedora 32 Update: squid-4.13-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Third Pa |
| [security-announce] openSUSE-SU-2020:1346-1: critical: Security update f                 | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           | Mailing  |
| [SECURITY] [DLA 2394-1] squid3 security update                                           | MLIST   | <a href="https://lists.debian.org">lists.debian.org</a>               | Mailing  |
| USN-4551-1: Squid vulnerabilities   Ubuntu security notices   Ubuntu                     | UBUNTU  | <a href="https://usn.ubuntu.com">usn.ubuntu.com</a>                   | Third Pa |
| USN-4477-1: Squid vulnerabilities   Ubuntu security notices   Ubuntu                     | UBUNTU  | <a href="https://usn.ubuntu.com">usn.ubuntu.com</a>                   | Third Pa |
| [SECURITY] Fedora 31 Update: squid-4.13-1.fc31 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |          |
| September 2020 Squid Vulnerabilities in NetApp Products   NetApp Product Security        | CONFIRM | <a href="https://security.netapp.com">security.netapp.com</a>         | Third Pa |
| [SECURITY] Fedora 32 Update: squid-4.13-1.fc32 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |          |
| August 2020 Squid Vulnerabilities in NetApp Products   NetApp Product Security           | CONFIRM | <a href="https://security.netapp.com">security.netapp.com</a>         | Third Pa |
| [security-announce] openSUSE-SU-2020:1369-1: critical: Security update f                 | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           | Mailing  |
| [SECURITY] Fedora 33 Update: squid-4.13-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Third Pa |
| CVE Program record                                                                       | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                         | canonic  |
| NVD vulnerability detail                                                                 | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                       | canonic  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[356259](#) Amazon Linux Security Advisory for squid : ALASSQUID4-2023-006

[376993](#) Alibaba Cloud Linux Security Update for squid (ALINUX2-SA-2020:0119)

[377360](#) Alibaba Cloud Linux Security Update for squid:4 (ALINUX3-SA-2022:0124)

[500659](#) Alpine Linux Security Update for squid

[501495](#) Alpine Linux Security Update for squid

[504429](#) Alpine Linux Security Update for squid

[753154](#) SUSE Enterprise Linux Security Update for squid (SUSE-SU-2022:14908-1)

[960348](#) Rocky Linux Security Update for squid:4 (RLSA-2020:3623)

© [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](#)**