



# CVE-2019-18676

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-18676
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-26 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:06:00 UTC
<b>Description</b>	An issue was discovered in Squid 3.x and 4.x through 4.8. Due to incorrect input validation, there is a heap-based buffer ov

## Risk And Classification

**Problem Types:** CWE-787

## 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>	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>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	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>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	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>	30	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>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	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

[www.squid-cache.org/Versions/v4/changesets/squid-4-fb9df75efd7a5cc244b4886a9d42ea...](http://www.squid-cache.org/Versions/v4/changesets/squid-4-fb9df75efd7a5cc244b4886a9d42ea...)

[SECURITY] [DLA 2278-1] squid3 security update

Update URI parser to use SBuf parsing APIs by yadij · Pull Request #275 · squid-cache/squid · GitHub

[SECURITY] Fedora 30 Update: squid-4.9-2.fc30 - package-announce - Fedora Mailing-Lists

USN-4446-1: Squid vulnerabilities | Ubuntu security notices | Ubuntu

USN-4213-1: Squid vulnerabilities | Ubuntu security notices | Ubuntu

[SECURITY] Fedora 31 Update: squid-4.9-2.fc31 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 31 Update: squid-4.9-2.fc31 - package-announce - Fedora Mailing-Lists

Debian -- Security Information -- DSA-4682-1 squid

[SECURITY] Fedora 30 Update: squid-4.9-2.fc30 - package-announce - Fedora Mailing-Lists

Bug 1156329 – VUL-0: CVE-2019-12523,CVE-2019-18676: squid,squid3: improper input validation can lead to access to restricted HTTP ser

[www.squid-cache.org/Advisories/SQUID-2019\\_8.txt](http://www.squid-cache.org/Advisories/SQUID-2019_8.txt)

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159658](#) Oracle Enterprise Linux Security Update for squid:4 (ELSA-2020-4743)

[296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)

[355319](#) Amazon Linux Security Advisory for squid : ALAS2-2023-2065

[355348](#) Amazon Linux Security Advisory for squid : ALAS-2023-1757

[356277](#) Amazon Linux Security Advisory for squid : ALASSQUID4-2023-007

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

[670223](#) EulerOS Security Update for squid (EulerOS-SA-2021-1852)

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

[940034](#) AlmaLinux Security Update for squid:4 (ALSA-2020:4743)

[960867](#) Rocky Linux Security Update for squid:4 (RLSA-2020:4743)

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](https://status.cve.report)**