



# CVE-2019-18678

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

## Summary

<b>CVE</b>	CVE-2019-18678
<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. It allows attackers to smuggle HTTP requests through frontend s

## 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>	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>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	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	Source
[SECURITY] [DLA 2278-1] squid3 security update	MLIST
[SECURITY] Fedora 30 Update: squid-4.9-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
Squid: Multiple vulnerabilities (GLSA 202003-34) — Gentoo security	GENTOO
www.squid-cache.org/Versions/v4/changesets/squid-4-671ba97abe929156dc4c717ee52ad2...	CONFIRM
RFC 7230: server MUST reject messages with BWS after field-name by yadij · Pull Request #445 · squid-cache/squid · GitHub	MISC
Bug 1156323 – VUL-0: CVE-2019-18678: squid,squid3: incorrect message parsing leads to HTTP request splitting issue	CONFIRM
USN-4213-1: Squid vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU
[SECURITY] Fedora 31 Update: squid-4.9-2.fc31 - package-announce - Fedora Mailing-Lists	
[SECURITY] [DLA 2028-1] squid3 security update	MLIST
[SECURITY] Fedora 31 Update: squid-4.9-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
Debian -- Security Information -- DSA-4682-1 squid	DEBIAN
[SECURITY] Fedora 30 Update: squid-4.9-2.fc30 - package-announce - Fedora Mailing-Lists	
www.squid-cache.org/Advisories/SQUID-2019_10.txt	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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)
- 356277 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-007
- 356430 Amazon Linux Security Advisory for squid : ALAS2-2023-2318
- 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](https://status.cve.report)**