



# CVE-2021-31806

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

## Summary

<b>CVE</b>	CVE-2021-31806
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-27 13:15:00 UTC
<b>Updated</b>	2023-11-07 03:35:00 UTC
<b>Description</b>	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. Due to a memory-management bug, it is vulnerable to a

## Risk And Classification

**Problem Types:** CWE-116

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Manager</a>	-	All	All	All
Application	<a href="#">Squid-cache</a>	<a href="#">Squid</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 33 Update: squid-4.15-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
<a href="https://www.squid-cache.org/Versions/v4/changesets/squid-4-e7cf864f938f24eea8af0692c04d16...">www.squid-cache.org/Versions/v4/changesets/squid-4-e7cf864f938f24eea8af0692c04d16...</a>	MISC	<a href="https://www.squid-cache.org">www.squid-cache.org</a>	
June 2021 Squid Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
[SECURITY] Fedora 33 Update: squid-4.15-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Debian -- Security Information -- DSA-4924-1 squid	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
[SECURITY] [DLA 2685-1] squid3 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
SQUID-2021:4 Multiple Issues in HTTP Range header · Advisory · squid-cache/squid · GitHub	MISC	<a href="https://github.com">github.com</a>	
20231016 Squid Caching Proxy Security Audit: 55 Vulnerabilities, 35 0days.	FULLDISC	<a href="https://seclists.org">seclists.org</a>	

[SECURITY] Fedora 34 Update: squid-5.0.6-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 34 Update: squid-5.0.6-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
oss-security - Squid Caching Proxy Security Audit: 55 Vulnerabilities, 35 0days.	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [159409](#) Oracle Enterprise Linux Security Update for squid (ELSA-2021-9465)
- [159483](#) Oracle Enterprise Linux Security Update for squid:4 (ELSA-2021-4292)
- [178623](#) Debian Security Update for squid (DSA 4924-1)
- [178639](#) Debian Security Update for squid (DSA 4924-1)
- [178671](#) Debian Security Update for squid3 (DLA 2685-1)
- [179708](#) Debian Security Update for squid (CVE-2021-31806)
- [198400](#) Ubuntu Security Notification for Squid vulnerabilities (USN-4981-1)
- [239815](#) Red Hat Update for squid:4 security (RHSA-2021:4292)
- [281619](#) Fedora Security Update for squid (FEDORA-2021-c0bec55ec7)
- [281620](#) Fedora Security Update for squid (FEDORA-2021-24af72ff2c)
- [296065](#) Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)
- [354752](#) Amazon Linux Security Advisory for squid : ALAS-2023-1687
- [354783](#) Amazon Linux Security Advisory for squid : ALAS2-2023-1950
- [356184](#) Amazon Linux Security Advisory for squid : ALASSQUID4-2023-004
- [375570](#) Squid Multiple Denial Of Service Vulnerability (SQUID-2021:1,SQUID-2021:2,SQUID-2021:3,SQUID-2021:4,SQUID-2021:5)
- [500661](#) Alpine Linux Security Update for squid
- [500786](#) Alpine Linux Security Update for squid
- [501497](#) Alpine Linux Security Update for squid
- [502032](#) Alpine Linux Security Update for squid
- [504433](#) Alpine Linux Security Update for squid
- [670559](#) EulerOS Security Update for squid (EulerOS-SA-2021-2317)

<a href="#">670675</a> EulerOS Security Update for squid (EulerOS-SA-2021-2433)
<a href="#">670761</a> EulerOS Security Update for squid (EulerOS-SA-2021-2519)
<a href="#">670916</a> EulerOS Security Update for squid (EulerOS-SA-2021-2433)
<a href="#">670997</a> EulerOS Security Update for squid (EulerOS-SA-2021-2618)
<a href="#">710101</a> Gentoo Linux Squid Multiple vulnerabilities (GLSA 202105-14)
<a href="#">750098</a> SUSE Enterprise Linux Security Update for squid (SUSE-SU-2021:1838-1)
<a href="#">750160</a> SUSE Enterprise Linux Security Update for squid (SUSE-SU-2021:1961-1)
<a href="#">750641</a> OpenSUSE Security Update for squid (openSUSE-SU-2021:0879-1)
<a href="#">750782</a> OpenSUSE Security Update for squid (openSUSE-SU-2021:1961-1)
<a href="#">940500</a> AlmaLinux Security Update for squid:4 (ALSA-2021:4292)
<a href="#">960193</a> Rocky Linux Security Update for squid:4 (RLSA-2021:4292)

© [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](#)