



# CVE-2023-5824

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

## Summary

<b>CVE</b>	CVE-2023-5824
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-03 08:15:00 UTC
<b>Updated</b>	2024-01-25 18:15:00 UTC
<b>Description</b>	Squid is vulnerable to Denial of Service attack against HTTP and HTTPS clients due to an Improper Handling of Structural

## Risk And Classification

**Problem Types:** CWE-755

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Squid-cache</a>	<a href="#">Squid</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://security.netapp.com/advisory/ntap-20231130-0003">security.netapp.com/advisory/ntap-20231130-0003</a>		<a href="https://security.netapp.com">security.netapp.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
cve-details	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	
SQUID-2023:2 Multiple issues in HTTP response caching · Advisory · squid-cache/squid · GitHub	MISC	<a href="https://github.com">github.com</a>	
RHSA-2023:7465		<a href="https://access.redhat.com">access.redhat.com</a>	
2245914 – (CVE-2023-5824) CVE-2023-5824 squid: DoS against HTTP and HTTPS	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
RHSA-2023:7668		<a href="https://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	cano

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">161198</a> Oracle Enterprise Linux Security Update for squid (ELSA-2023-7465)
<a href="#">161218</a> Oracle Enterprise Linux Security Update for squid:4 (ELSA-2023-7668)
<a href="#">200247</a> Ubuntu Security Notification for Squid Vulnerabilities (USN-6728-1)
<a href="#">242506</a> Red Hat Update for squid (RHSA-2023:7465)
<a href="#">242549</a> Red Hat Update for squid:4 (RHSA-2023:7668)
<a href="#">242863</a> Red Hat Update for squid:4 (RHSA-2024:0397)
<a href="#">242910</a> Red Hat Update for squid (RHSA-2024:0072)
<a href="#">242913</a> Red Hat Update for squid:4 (RHSA-2024:0773)
<a href="#">242914</a> Red Hat Update for squid:4 (RHSA-2024:0771)
<a href="#">242915</a> Red Hat Update for squid:4 (RHSA-2024:0772)
<a href="#">243018</a> Red Hat Update for squid (RHSA-2024:1153)
<a href="#">296108</a> Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
<a href="#">357373</a> Amazon Linux Security Advisory for squid : ALAS2023-2024-578
<a href="#">379621</a> Alibaba Cloud Linux Security Update for squid:4 (ALINUX3-SA-2024:0020)
<a href="#">941421</a> AlmaLinux Security Update for squid (ALSA-2023:7465)
<a href="#">941492</a> AlmaLinux Security Update for squid:4 (ALSA-2023:7668)
<a href="#">961086</a> Rocky Linux Security Update for squid:4 (RLSA-2023:7668)

© 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](#)**