



CVE-2023-46847

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

Summary

CVE	CVE-2023-46847
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 08:15:00 UTC
Updated	2023-11-30 22:15:00 UTC
Description	Squid is vulnerable to a Denial of Service, where a remote attacker can perform buffer overflow attack by writing up to 2 ME

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.8	All	All	All
Operating System	Redhat	Enterprise Linux Eus	9.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	9.2	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	9.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.8	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	9.2	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

Application	Squid-cache	Squid	All	All	All	All
-------------	-------------	-------	-----	-----	-----	-----

References

Reference	Source	Link
Red Hat		access.redhat.com
RHSA-2023:7576		access.redhat.com
Red Hat	MISC	access.redhat.com
Red Hat		access.redhat.com
Red Hat	MISC	access.redhat.com
Red Hat	MISC	access.redhat.com
2245916 – (CVE-2023-46847) CVE-2023-46847 squid: Denial of Service in HTTP Digest Authentication	MISC	bugzilla.redhat.com
Red Hat		access.redhat.com
SQUID-2023:3 Denial of Service in HTTP Digest Authentication · Advisory · squid-cache/squid · GitHub	MISC	github.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
security.netapp.com/advisory/ntap-20231130-0002		security.netapp.com
RHSA-2023:7578		access.redhat.com
Red Hat		access.redhat.com
cve-details	MISC	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161045 Oracle Enterprise Linux Security Update for squid (ELSA-2023-6266)
161050 Oracle Enterprise Linux Security Update for squid:4 (ELSA-2023-6267)
161052 Oracle Enterprise Linux Security Update for squid (ELSA-2023-6805)
161091 Oracle Enterprise Linux Security Update for squid (ELSA-2023-6748)
161191 Oracle Enterprise Linux Security Update for squid:4 (ELSA-2023-7213)
161285 Oracle Enterprise Linux Security Update for squid34 (ELSA-2023-6882)

161286 Oracle Enterprise Linux Security Update for squid (ELSA-2023-6884)
199932 Ubuntu Security Notification for Squid Vulnerabilities (USN-6500-1)
199990 Ubuntu Security Notification for Squid Vulnerabilities (USN-6500-2)
242271 Red Hat Update for squid (RHSA-2023:6266)
242272 Red Hat Update for squid:4 (RHSA-2023:6267)
242276 Red Hat Update for squid (RHSA-2023:6268)
242289 Red Hat Update for squid (RHSA-2023:6748)
242337 Red Hat Update for squid:4 (RHSA-2023:6803)
242339 Red Hat Update for squid:4 (RHSA-2023:6804)
242382 Red Hat Update for squid:4 (RHSA-2023:6810)
242389 Red Hat Update for squid:4 (RHSA-2023:6801)
242390 Red Hat Update for squid (RHSA-2023:6805)
242439 Red Hat Update for squid:4 (RHSA-2023:7213)
257262 Centos Security Update for squid
257292 CentOS Security Update for squid (CESA-2023:6805)
296108 Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
356512 Amazon Linux Security Advisory for squid : ALAS2023-2023-402
356552 Amazon Linux Security Advisory for squid : ALAS-2023-1872
356984 Amazon Linux Security Advisory for squid : AL2012-2023-468
379040 Alibaba Cloud Linux Security Update for squid (ALINUX2-SA-2023:0045)
379044 Alibaba Cloud Linux Security Update for squid:4 (ALINUX3-SA-2023:0135)
505941 Alpine Linux Security Update for squid
6000513 Debian Security Update for squid (DSA 5637-1)
755236 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2023:4381-1)
755237 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2023:4380-1)
755241 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2023:4384-1)
941335 AlmaLinux Security Update for squid (ALSA-2023:6266)
941342 AlmaLinux Security Update for squid:4 (ALSA-2023:6267)

941397 AlmaLinux Security Update for squid (ALSA-2023:6748)
941468 AlmaLinux Security Update for squid:4 (ALSA-2023:7213)
961066 Rocky Linux Security Update for squid:4 (RLSA-2023:6267)
961070 Rocky Linux Security Update for squid (RLSA-2023:6266)
961075 Rocky Linux Security Update for squid:4 (RLSA-2023:7213)

© [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](#)