



CVE-2022-39173

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-39173
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-29 01:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	In wolfSSL before 5.5.1, malicious clients can cause a buffer overflow during a TLS 1.3 handshake. This occurs when an at

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wolfssl	Wolfssl	All	All	All	All

References

Reference	Source	Link
wolfSSL Security Vulnerabilities Documentation – wolfSSL	MISC	www.wolfssl.com
Keeping the wolves out of wolfSSL Trail of Bits Blog	MISC	blog.trailofbits.com
Releases · wolfSSL/wolfssl · GitHub	MISC	github.com
Full Disclosure: wolfssl before 5.5.1: CVE-2022-39173 Buffer overflow when refining cipher suites	FULLDISC	seclists.org
wolfSSL Buffer Overflow ≈ Packet Storm	MISC	packetstormsecurity.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

[183341](#) Debian Security Update for wolfssl (CVE-2022-39173)

[502968](#) Alpine Linux Security Update for wolfssl

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)