CVE-2022-39173

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

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

505834 Alpine Linux Security Update for wolfssl

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report