CVE-2022-38152

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

Summary

CVE	CVE-2022-38152
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-31 17:15:00 UTC
Updated	2023-03-01 15:50:00 UTC
Description	An issue was discovered in wolfSSL before 5.5.0. When a TLS 1.3 client connects to a wolfSSL server and SSL_clear is ca

Risk And Classification

Problem Types: CWE-754

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Sourc
wolfSSL Security Vulnerabilities | Documentation – wolfSSL	CONF
Keeping the wolves out of wolfSSL | Trail of Bits Blog	MISC
Fixes to better handle re-use of a WOLFSSL object via wolfSSL_clear by SparkiDev · Pull Request #5468 · wolfSSL/wolfssl · GitHub	MISC
wolfSSL Session Resumption Denial Of Service ≈ Packet Storm	MISC
Releases · wolfSSL/wolfssl · GitHub	MISC
Full Disclosure: wolfSSL before 5.5.0: Denial-of-service with session resumption	FULLD
GitHub - tlspuffin/tlspuffin: A symbolic-model-guided fuzzer for TLS	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184277 Debian Security Update for wolfssl (CVE-2022-38152)

502967 Alpine Linux Security Update for wolfssl

505833 Alpine Linux Security Update for wolfssl

Free CVE JSON API cve.report/api

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