CVE-2022-38153

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

Summary

CVE	CVE-2022-38153
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-31 18:15:00 UTC
Updated	2023-03-01 15:51:00 UTC
Description	An issue was discovered in wolfSSL before 5.5.0 (when --enable-session-ticket is used); however, only version 5.3.0 is exp

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wolfssl	Wolfssl	5.3.0	All	All	All

References

Reference
GitHub - trailofbits/tlspuffin: A symbolic-model-guided fuzzer for TLS
wolfSSL Security Vulnerabilities | Documentation – wolfSSL
Keeping the wolves out of wolfSSL | Trail of Bits Blog
wolfSSL 5.3.0 Denial Of Service ≈ Packet Storm
Releases · wolfSSL/wolfssl · GitHub
Full Disclosure: wolfSSL 5.3.0: Denial-of-service
Remove WOLFSSL_SESSION_TYPE_REF buffers from WOLFSSL_SESSION by julek-wolfssl · Pull Request #5476 · wolfSSL/wolfssl · GitHu
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

182584 Debian Security Update for wolfssl (CVE-2022-38153)