CVE-2022-23408

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-23408
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-18 21:15:00 UTC
Updated	2022-01-27 20:03:00 UTC
Description	wolfSSL 5.x before 5.1.1 uses non-random IV values in certain situations. This affects connections (without AEAD) using AI

Risk And Classification

Problem Types: CWE-330

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	Tags
fix for location of xmemset by JacobBarthelmeh · Pull Request #4710 · wolfSSL/wolfssl · GitHub	MISC	github.com	
wolfssl/ChangeLog.md at master · wolfSSL/wolfssl · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

182330 Debian Security Update for wolfssl (CVE-2022-23408)

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