CVE-2022-42905

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

Summary

CVE	CVE-2022-42905
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-07 00:15:00 UTC
Updated	2023-02-15 22:15:00 UTC
Description	In wolfSSL before 5.5.2, if callback functions are enabled (via the WOLFSSL_CALLBACKS flag), then a malicious TLS 1.3

Risk And Classification

Problem Types: CWE-125

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
wolfSSL WOLFSSL_CALLBACKS Heap Buffer Over-Read ≈ Packet Storm	MISC	packetstormsecurity.com	
Full Disclosure: wolfSSL before 5.5.2: Heap-buffer over-read with WOLFSSL_CALLBACKS	FULLDISC	seclists.org	
wolfSSL Security Vulnerabilities | Documentation – wolfSSL	MISC	www.wolfssl.com	
Release wolfSSL Release 5.5.2 (Oct 28, 2022) · wolfSSL/wolfssl · GitHub	MISC	github.com	
Keeping the wolves out of wolfSSL | Trail of Bits Blog	MISC	blog.trailofbits.com	
Releases · wolfSSL/wolfssl · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181984 Debian Security Update for wolfssl (CVE-2022-42905)

502969 Alpine Linux Security Update for wolfssl

505835 Alpine Linux Security Update for wolfssl

905128 Common Base Linux Mariner (CBL-Mariner) Security Update for mariadb (12563)

Free CVE JSON API cve.report/api

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