CVE-2023-3724

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

Summary

CVE	CVE-2023-3724
State	PUBLIC
Assigner	facts@wolfssl.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-17 22:15:00 UTC
Updated	2023-07-28 13:54:00 UTC
Description	If a TLS 1.3 client gets neither a PSK (pre shared key) extension nor a KSE (key share extension) when connecting to a ma

Risk And Classification

Problem Types: CWE-295

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
add tls extension sanity check by JacobBarthelmeh · Pull Request #6412 · wolfSSL/wolfssl · GitHub	MISC	github.com	
wolfSSL Security Vulnerabilities | Documentation – wolfSSL	MISC	www.wolfssl.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

503279 Alpine Linux Security Update for wolfssl

506275 Alpine Linux Security Update for wolfssl

907217 Common Base Linux Mariner (CBL-Mariner) Security Update for mariadb (27649-1)

Free CVE JSON API cve.report/api

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