CVE-2022-25638

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

Summary

CVE	CVE-2022-25638
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-24 15:15:00 UTC
Updated	2022-03-04 16:48:00 UTC
Description	In wolfSSL before 5.2.0, certificate validation may be bypassed during attempted authentication by a TLS 1.3 client to a TLS

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	Sou
Fix for mutual authentication to prevent mismatch of certificate and sigalgo by dgarske · Pull Request #4813 · wolfSSL/wolfssl · GitHub	MIS
wolfSSL Security Vulnerabilities | Documentation – wolfSSL	CON
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179196 Debian Security Update for wolfssl (CVE-2022-25638)

Free CVE JSON API cve.report/api

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