CVE-2021-3336

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3336
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-29 05:15:00 UTC
Updated	2021-03-04 21:20:00 UTC
Description	DoTls13CertificateVerify in tls13.c in wolfSSL before 4.7.0 does not cease processing for certain anomalous peer behavior

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
Application	Wolfssl	Wolfssl	All	All	All	All

References

Reference	Source	Link
TLS 1.3: ensure key for signature in CertificateVerify by SparkiDev · Pull Request #3676 · wolfSSL/wolfssl · GitHub	MISC	github.com
wolfSSL Security Vulnerabilities | wolfSSL Embedded SSL/TLS Library	CONFIRM	www.wolfs
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179418 Debian Security Update for wolfssl (CVE-2021-3336)

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