CVE-2019-19962

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-19962
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-25 00:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	wolfSSL before 4.3.0 mishandles calls to wc_SignatureGenerateHash, leading to fault injection in RSA cryptography.

Risk And Classification

Problem Types: CWE-347

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	Tags
Change signature generation to verify by default · wolfSSL/wolfssl@2387851 · GitHub	MISC	github.com	Patch, Third Party Advis
Release wolfSSL release version 4.3.0 · wolfSSL/wolfssl · GitHub	MISC	github.com	Release Notes, Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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