CVE-2020-12457

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-12457
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-21 14:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	An issue was discovered in wolfSSL before 4.5.0. It mishandles the change_cipher_spec (CCS) message processing logic

Risk And Classification

Problem Types: CWE-835

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	Li
Release wolfSSL Release 4.5.0 (08/19/2020) · wolfSSL/wolfssl · GitHub	CONFIRM	git
In TLS 1.3, don't allow multiple ChangeCipherSpecs in a row by SparkiDev · Pull Request #2927 · wolfSSL/wolfssl · GitHub	MISC	git
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180739 Debian Security Update for wolfssl (CVE-2020-12457)

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