CVE-2021-38597

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-38597
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-12 15:15:00 UTC
Updated	2021-08-23 14:07:00 UTC
Description	wolfSSL before 4.8.1 incorrectly skips OCSP verification in certain situations of irrelevant response data that contains the N

Risk And Classification

Problem Types: CWE-345

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
wolfSSL Changelog | wolfSSL Embedded SSL/TLS Library Documentation	MISC	www.wolfssl.com	
OCSP: improve handling of OCSP no check extension · wolfSSL/wolfssl@f93083b · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179415 Debian Security Update for wolfssl (CVE-2021-38597)

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