



CVE-2019-19960

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-19960
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-25 00:15:00 UTC
Updated	2020-01-02 19:37:00 UTC
Description	In wolfSSL before 4.3.0, wc_ecc_mulmod_ex does not properly resist side-channel attacks.

Risk And Classification

Problem Types: NVD-CWE-Other

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
Release wolfSSL release version 4.3.0 · wolfSSL/wolfssl · GitHub	MISC	github.com	Release Note
Merge pull request #2637 from SparkiDev/ecc_cache_resist · wolfSSL/wolfssl@5ee9f9c · GitHub	MISC	github.com	Patch, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

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 registered 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](#)