Fault injection attack with ML-DSA and ML-KEM on ARM

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-3503
State	PUBLISHED
Assigner	wolfSSL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-19 19:16:20 UTC
Updated	2026-04-29 17:28:53 UTC
Description	Protection mechanism failure in wolfCrypt post-quantum implementations (ML-KEM and ML-DSA) in wolfSSL on ARM Cort

Risk And Classification

Primary CVSS: v4.0 4.3 MEDIUM from facts@wolfssl.com

CVSS:4.0/AV:P/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:Amber

EPSS: 0.000080000 probability, percentile 0.006920000 (date 2026-05-05)

Problem Types: CWE-335 | CWE-335 CWE-335 Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	4.3	MEDIUM	CVSS:4.0/AV:P/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/C.
4.0	CNA	CVSS	4.3	MEDIUM	CVSS:4.0/AV:P/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:N/U:Amb
3.1	nvd@nist.gov	Primary	5.2	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:P/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:Amber

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

Low

Availability

None

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wolfssl	Wolfssl	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WolfSSL Inc.	WolfSSL WolfCrypt	affected 5.8.2 5.9.0 semver	ARM

References

Reference	Source	Link	Tags
github.com/wolfSSL/wolfssl/pull/9734	facts@wolfssl.com	github.com	Issue Tracking, Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Hariprasad Kelassery Valsaraj of Temasek Laboratories (en)

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