Stack Buffer Overflow in wolfSSL PKCS7 wc_PKCS7_DecryptOri() via Oversized OID

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

Summary

CVE	CVE-2026-5295
State	PUBLISHED
Assigner	wolfSSL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 23:17:01 UTC
Updated	2026-04-29 14:08:46 UTC
Description	A stack buffer overflow exists in wolfSSL's PKCS7 implementation in the wc_PKCS7_DecryptOri() function in wolfcrypt/src/

Risk And Classification

Primary CVSS: v4.0 5.9 MEDIUM from facts@wolfssl.com

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:H/SC:N/SI:N/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:X

EPSS: 0.000170000 probability, percentile 0.040680000 (date 2026-05-01)

Problem Types: CWE-121 | CWE-121 CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	5.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:X/C.
4.0	CNA	CVSS	5.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:H/SC:N/SI:N/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:X

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

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	WolfSSL	affected 5.9.1 semver	Not specified

References

Reference	Source	Link	Tags
github.com/wolfSSL/wolfssl/pull/10116	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: Sunwoo Lee, (Korea Institute of Energy Technology, KENTECH) (en)

CNA: Woohyun Choi, (Korea Institute of Energy Technology, KENTECH) (en)

CNA: Seunghyun Yoon, (Korea Institute of Energy Technology, KENTECH) (en)

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