



# Stack Buffer Overflow in wolfSSL PKCS7 wc\_PKCS7\_DecryptOri() via Oversized OID

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

## Summary

<b>CVE</b>	CVE-2026-5295
<b>State</b>	PUBLISHED
<b>Assigner</b>	wolfSSL
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-09 23:17:01 UTC
<b>Updated</b>	2026-04-29 14:08:46 UTC
<b>Description</b>	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/MSX/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/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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/MSX/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
CVE	Wolfssl	Wolfssl	1.5.0	Linux, Windows

CNA      WolfSSL      WolfSSL      affected 5.9.1 semver      Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/wolfSSL/wolfssl/pull/10116">github.com/wolfSSL/wolfssl/pull/10116</a>	facts@wolfssl.com	<a href="https://github.com">github.com</a>	Issue Tracking, Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)