wolfSSL heap OOB read in PKCS7 SignedData streaming

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

Summary

CVE	CVE-2026-5392
State	PUBLISHED
Assigner	wolfSSL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 00:16:35 UTC
Updated	2026-04-29 14:02:43 UTC
Description	Heap out-of-bounds read in PKCS7 parsing. A crafted PKCS7 message can trigger an OOB read on the heap. The missing

Risk And Classification

Primary CVSS: v4.0 2.3 LOW from facts@wolfssl.com

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/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: 0.000140000 probability, percentile 0.025190000 (date 2026-05-01)

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	2.3	LOW	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/C.
4.0	CNA	CVSS	2.3	LOW	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

Low

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

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/10039	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: J Laratro (d0sf3t) (en)

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