Stack buffer overflow in PKCS7 SignedData encoding with custom signed attributes

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

Summary

CVE	CVE-2026-0819
State	PUBLISHED
Assigner	wolfSSL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-19 17:16:21 UTC
Updated	2026-04-29 18:50:05 UTC
Description	A stack buffer overflow vulnerability exists in wolfSSL's PKCS7 SignedData encoding functionality. In wc_PKCS7_BuildSigr

Risk And Classification

Primary CVSS: v4.0 2.2 LOW from facts@wolfssl.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/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: 0.000180000 probability, percentile 0.048750000 (date 2026-05-02)

Problem Types: CWE-121 | CWE-787 | CWE-121 CWE-121: Stack-based Buffer Overflow | CWE-787 CWE-787: Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	2.2	LOW	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/C.
4.0	CNA	CVSS	2.2	LOW	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:U
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/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

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/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 5.5.0 5.9.0 semver	Not specified

References

Reference	Source	Link	Tags
github.com/wolfSSL/wolfssl/pull/9630	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: Maor Caplan (en)

Additional Advisory Data

Solutions

CNA: Update to the patched version of wolfSSL. The fix adds proper bounds checking in wc_PKCS7_BuildSignedAttributes() to validate that the number of custom signed attributes does not exceed the available space in the fixed-size signedAttribs array, returning BUFFER_E if the limit is exceeded.

Workarounds

CNA: Ensure that applications using wolfSSL PKCS7 signing functionality validate and limit the number of custom signed attributes (signedAttribsSz) to no more than MAX_SIGNED_ATTRIBS_SZ (default 7) minus the number of default signed attributes enabled. Do not allow untrusted input to control the signedAttribs array or its size.

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