Buffer overflow in CRL number parsing in wolfSSL

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

Summary

CVE	CVE-2026-3548
State	PUBLISHED
Assigner	wolfSSL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-19 18:16:22 UTC
Updated	2026-04-29 18:41:38 UTC
Description	Two buffer overflow vulnerabilities existed in the wolfSSL CRL parser when parsing CRL numbers: a heap-based buffer ove

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from facts@wolfssl.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/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: 0.000330000 probability, percentile 0.096040000 (date 2026-05-05)

Problem Types: CWE-122 | CWE-787 | CWE-787 CWE-787 Out-of-bounds Write | CWE-122 CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/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 5.9.0 semver	MacOS, Linux, Windows

References

Reference	Source	Link	Tags
github.com/wolfSSL/wolfssl/pull/9873	facts@wolfssl.com	github.com	Exploit, Issue Tracking, Patch
github.com/wolfSSL/wolfssl/pull/9628	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

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Workarounds

CNA: Disabling CRL processing is the only effective workaround for this issue. Preventing the overflow by validating the CRL number length requires source code modification and therefore should be considered a fix rather than a workaround.

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