



# wolfSSL ECDSA Certificate Verification

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-5194
<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 20:16:28 UTC
<b>Updated</b>	2026-04-16 20:37:11 UTC
<b>Description</b>	Missing hash/digest size and OID checks allow digests smaller than allowed when verifying ECDSA certificates, or smaller

## Risk And Classification

**Primary CVSS:** v4.0 9.3 CRITICAL from facts@wolfssl.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:H/SI:L/SA:L/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:Re d

**EPSS:** 0.000360000 probability, percentile 0.104340000 (date 2026-04-16)

**Problem Types:** CWE-295 | CWE-295 CWE-295 Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:H/SI:L/SA:L/E:X/C
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:H/SI:L/SA:L/U:Rec
3.1	nvd@nist.gov	Primary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality: **High**

Integrity: **High**

Availability: **Low**

Sub Conf.: **High**

Sub Integrity: **Low**

Sub Availability: **Low**

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

CVSS v3.1 Breakdown

Attack Vector: **Network**

Attack Complexity: **Low**

Privileges Required: **None**

User Interaction: **None**

Scope: **Unchanged**

Confidentiality: **High**

Integrity: **High**

Availability: **None**

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

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	<a href="#">WolfSSL</a>	<a href="#">WolfSSL</a>	affected 3.12.0 5.9.1 semver	Not specified
-----	-------------------------	-------------------------	------------------------------	---------------

## References

Reference	Source	Link	Tags
<a href="https://github.com/wolfSSL/wolfssl/pull/10131">github.com/wolfSSL/wolfssl/pull/10131</a>	<a href="mailto:facts@wolfssl.com">facts@wolfssl.com</a>	<a href="https://github.com">github.com</a>	Issue Tracking
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:** Nicholas Carlini from Anthropic (en)

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**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)