



# wolfSSL ARIA-GCM TLS 1.2/DTLS 1.2 GCM nonce reuse

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

## Summary

<b>CVE</b>	CVE-2026-5446
<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 21:16:12 UTC
<b>Updated</b>	2026-04-09 21:16:12 UTC
<b>Description</b>	In wolfSSL, ARIA-GCM cipher suites used in TLS 1.2 and DTLS 1.2 reuse an identical 12-byte GCM nonce for every applic

## Risk And Classification

**Primary CVSS:** v4.0 6 MEDIUM from facts@wolfssl.com

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

**Problem Types:** CWE-323 | CWE-323 CWE-323 Reusing a Nonce, Key Pair in Encryption

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:N/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	6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">WolfSSL</a>	<a href="#">WolfSSL</a>	affected 5.2.1 5.9.1 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="#">github.com/wolfSSL/wolfssl/pull/10111</a>	facts@wolfssl.com	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Calif.io in collaboration with Claude and Anthropic Research (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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)