



Heap buffer overflow in session parsing with wolfSSL_d2i_SSL_SESSION() function

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

Summary

CVE	CVE-2026-2646
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 18:42:47 UTC
Description	A heap-buffer-overflow vulnerability exists in wolfSSL's wolfSSL_d2i_SSL_SESSION() function. When deserializing session

Risk And Classification

Primary CVSS: v4.0 5 MEDIUM from facts@wolfssl.com

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

EPSS: 0.000340000 probability, percentile 0.098990000 (date 2026-05-05)

Problem Types: CWE-122 | CWE-787 | CWE-122 CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	facts@wolfssl.com	Secondary	5	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/C
4.0	CNA	CVSS	5	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/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
CVE	Wolfssl	Wolfssl	2.4.1-RC1	Linux, Windows

CNA	Wolfssl	Wolfssl	affected 5.8.4 semver	Not specified
References				
Reference	Source	Link	Tags	
github.com/wolfSSL/wolfssl/pull/9949	facts@wolfssl.com	github.com	Issue Tracking, Patch	
github.com/wolfSSL/wolfssl/pull/9748	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: Jonathan Bar Or (@yo_yo_yo_jbo) (en)				
CNA: Haruto Kimura (Stella) (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](#)