



# CVE-2022-42905

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

## Summary

<b>CVE</b>	CVE-2022-42905
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-07 00:15:00 UTC
<b>Updated</b>	2023-02-15 22:15:00 UTC
<b>Description</b>	In wolfSSL before 5.5.2, if callback functions are enabled (via the WOLFSSL_CALLBACKS flag), then a malicious TLS 1.3

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wolfssl	Wolfssl	All	All	All	All

## References

Reference	Source	Link	Tags
wolfSSL WOLFSSL_CALLBACKS Heap Buffer Over-Read ~ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
Full Disclosure: wolfSSL before 5.5.2: Heap-buffer over-read with WOLFSSL_CALLBACKS	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
wolfSSL Security Vulnerabilities   Documentation – wolfSSL	MISC	<a href="https://www.wolfssl.com">www.wolfssl.com</a>	
Release wolfSSL Release 5.5.2 (Oct 28, 2022) · wolfSSL/wolfssl · GitHub	MISC	<a href="https://github.com">github.com</a>	
Keeping the wolves out of wolfSSL   Trail of Bits Blog	MISC	<a href="https://blog.trailofbits.com">blog.trailofbits.com</a>	
Releases · wolfSSL/wolfssl · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

181984 Debian Security Update for wolfssl (CVE-2022-42905)

502969 Alpine Linux Security Update for wolfssl

505835 Alpine Linux Security Update for wolfssl

905128 Common Base Linux Mariner (CBL-Mariner) Security Update for mariadb (12563)

© [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](#)