



CVE-2023-3724

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-3724
State	PUBLIC
Assigner	facts@wolfssl.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-17 22:15:00 UTC
Updated	2023-07-28 13:54:00 UTC
Description	If a TLS 1.3 client gets neither a PSK (pre shared key) extension nor a KSE (key share extension) when connecting to a ma

Risk And Classification

Problem Types: CWE-295

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
add tls extension sanity check by JacobBarthelmeh · Pull Request #6412 · wolfSSL/wolfssl · GitHub	MISC	github.com	
wolfSSL Security Vulnerabilities Documentation – wolfSSL	MISC	www.wolfssl.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[503279](#) Alpine Linux Security Update for wolfssl

[506275](#) Alpine Linux Security Update for wolfssl

[907217](#) Common Base Linux Mariner (CBL-Mariner) Security Update for mariadb (27649-1)

© [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](#)