



CVE-2022-38152

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

Summary

CVE	CVE-2022-38152
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-31 17:15:00 UTC
Updated	2023-03-01 15:50:00 UTC
Description	An issue was discovered in wolfSSL before 5.5.0. When a TLS 1.3 client connects to a wolfSSL server and SSL_clear is ca

Risk And Classification

Problem Types: CWE-754

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
wolfSSL Security Vulnerabilities Documentation – wolfSSL	CONF
Keeping the wolves out of wolfSSL Trail of Bits Blog	MISC
Fixes to better handle re-use of a WOLFSSL object via wolfSSL_clear by SparkiDev · Pull Request #5468 · wolfSSL/wolfssl · GitHub	MISC
wolfSSL Session Resumption Denial Of Service ≈ Packet Storm	MISC
Releases · wolfSSL/wolfssl · GitHub	MISC
Full Disclosure: wolfSSL before 5.5.0: Denial-of-service with session resumption	FULLD
GitHub - tlspuffin/tlspuffin: A symbolic-model-guided fuzzer for TLS	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184277 Debian Security Update for wolfssl (CVE-2022-38152)

502967 Alpine Linux Security Update for wolfssl

505833 Alpine Linux Security Update for wolfssl

© [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](#)