



CVE-2022-38153

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

Summary

CVE	CVE-2022-38153
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-31 18:15:00 UTC
Updated	2023-03-01 15:51:00 UTC
Description	An issue was discovered in wolfSSL before 5.5.0 (when --enable-session-ticket is used); however, only version 5.3.0 is exp

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wolfssl	Wolfssl	5.3.0	All	All	All

References

Reference

- GitHub - trailofbits/tlspuffin: A symbolic-model-guided fuzzer for TLS
- wolfSSL Security Vulnerabilities | Documentation – wolfSSL
- Keeping the wolves out of wolfSSL | Trail of Bits Blog
- wolfSSL 5.3.0 Denial Of Service ≈ Packet Storm
- Releases · wolfSSL/wolfssl · GitHub
- Full Disclosure: wolfSSL 5.3.0: Denial-of-service
- Remove WOLFSSL_SESSION_TYPE_REF buffers from WOLFSSL_SESSION by julek-wolfssl · Pull Request #5476 · wolfSSL/wolfssl · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)