



CVE-2015-6925

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

Summary

CVE	CVE-2015-6925
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-22 15:59:00 UTC
Updated	2016-01-25 18:21:00 UTC
Description	wolfSSL (formerly CyaSSL) before 3.6.8 allows remote attackers to cause a denial of service (resource consumption or traf

Risk And Classification

Problem Types: CWE-399

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
GitHub - IAIK/wolfSSL-DoS: Proof of concept for denial of service attack on wolfSSL's DTLS server implementation.	MISC	github.com
Two Vulnerabilities Recently Found, An Attack on RSA using CRT and DoS Vulnerability With DTLS	CONFIRM	wolfssl.com
Docs-wolfssl-changelog	CONFIRM	wolfssl.com
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[690337](#) Free Berkeley Software Distribution (FreeBSD) Security Update for Wolf Secure Sockets Layer (wolfssl) (3d1372e1-7822-4fd8-b56e-5ee832afb96)

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