



CVE-2020-36177

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

Summary

CVE	CVE-2020-36177
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-06 16:15:00 UTC
Updated	2021-01-12 14:39:00 UTC
Description	RsaPad_PSS in wolfcrypt/src/rsa.c in wolfSSL before 4.6.0 has an out-of-bounds write for certain relationships between key

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Li
26567 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bu
RSA-PSS: Handle edge case with encoding message to hash · wolfSSL/wolfssl@fb2288c · GitHub	MISC	gi
Release wolfSSL release version 4.6.0 · wolfSSL/wolfssl · GitHub	MISC	gi
RSA-PSS: Handle edge case with encoding message to hash by SparkiDev · Pull Request #3426 · wolfSSL/wolfssl · GitHub	MISC	gi
Merge pull request #3426 from SparkiDev/rsa_pss_fix · wolfSSL/wolfssl@63bf5dc · GitHub	MISC	gi
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180794](#) Debian Security Update for wolfssl (CVE-2020-36177)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)