



CVE-2020-11713

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

Summary

CVE	CVE-2020-11713
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-12 17:15:00 UTC
Updated	2022-01-01 18:45:00 UTC
Description	wolfSSL 4.3.0 has mulmod code in wc_ecc_mulmod_ex in ecc.c that does not properly resist timing side-channel attacks.

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wolfssl	Wolfssl	4.3.0	All	All	All
Application	Wolfssl	Wolfssl	4.3.0	All	All	All

References

Reference	S
Change constant time and cache resistant ECC mulmod by SparkiDev · Pull Request #2894 · wolfSSL/wolfssl · GitHub	M
PoC for CVE-2020-11713. Timing side-channel on wc_ecc_mulmod which allows to recover private key used to sign messages. · GitHub	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180686](#) Debian Security Update for wolfssl (CVE-2020-11713)

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](#)