CVE-2020-11735

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-11735
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-25 14:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	The private-key operations in ecc.c in wolfSSL before 4.4.0 do not use a constant-time modular inverse when mapping to a

Risk And Classification

Problem Types: CWE-203

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	Link	Tags
Constant time EC map to affine for private operations · wolfSSL/wolfssl@1de07da · GitHub	CONFIRM	github.com	Patch, Third Party A
Release wolfSSL Release 4.4.0 (04/22/2020) · wolfSSL/wolfssl · GitHub	CONFIRM	github.com	Release Notes, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180737 Debian Security Update for wolfssl (CVE-2020-11735)

CVE.report and Source URL Uptime Status status.cve.report