



# CVE-2020-11735

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

## Summary

<b>CVE</b>	CVE-2020-11735
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-25 14:15:00 UTC
<b>Updated</b>	2021-07-21 11:39:00 UTC
<b>Description</b>	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	<a href="#">Wolfssl</a>	<a href="#">Wolfssl</a>	All	All	All	All
Application	<a href="#">Wolfssl</a>	<a href="#">Wolfssl</a>	All	All	All	All

## References

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

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

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](#)**