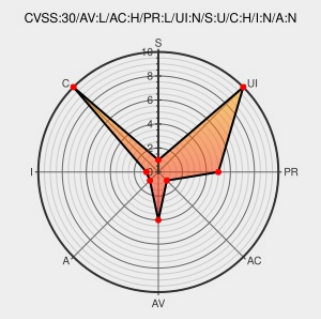
CVE-2018-12436

Published on: 06/14/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:23 PM UTC

CVE-2018-12436

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wolfssl from Wolfssl contain the following vulnerability:

wolfcrypt/src/ecc.c in wolfSSL before 3.15.1.patch allows a memory-cache side-channel attack on ECDSA signatures, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.

CVE-2018-12436 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Change ECDSA signing to use blinding. · wolfSSL/wolfssl@9b9568d · GitHub	Patch Third Party Advisory github.com	MISC github.com/wolfSSL/wolfssl/commit/9b9568d500f31f964af26ba8d01e542e1f27e5ca

GitHub	text/html	
wolfSSL and ROHNP - wolfSSL	Vendor Advisory www.wolfssl.com text/html	MISC www.wolfssl.com/wolfssh-and-rohnp/
No Description Provided	Third Party Advisory www.nccgroup.trust text/html	MISC www.nccgroup.trust/us/our-research/technical-advisory-return-of-the-hidden-number-problem/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:wolfssl:wolfssl:*:*:*:*:*:*:*:*:

cpe:2.3:a:wolfssl:wolfssl:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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