



CVE-2017-13099

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

Summary

CVE	CVE-2017-13099
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-13 01:29:00 UTC
Updated	2019-10-09 23:23:00 UTC
Description	wolfSSL prior to version 3.12.2 provides a weak Bleichenbacher oracle when any TLS cipher suite using RSA key exchange

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arubanetworks	Instant	All	All	All	All
Application	Arubanetworks	Instant	All	All	All	All
Hardware	Siemens	Scalance W1750d	-	All	All	All
Hardware	Siemens	Scalance W1750d	-	All	All	All
Operating System	Siemens	Scalance W1750d Firmware	All	All	All	All
Operating System	Siemens	Scalance W1750d Firmware	All	All	All	All
Application	Wolfssl	Wolfssl	All	All	All	All
Application	Wolfssl	Wolfssl	All	All	All	All

References

Reference	Source
wolfSSL CVE-2017-13099 Information Disclosure Vulnerability	BID
www.arubanetworks.com/assets/alert/ARUBA-PSA-2018-002.txt	CC
The ROBOT Attack - Return of Bleichenbacher's Oracle Threat	ML
cert-portal.siemens.com/productcert/pdf/ssa-464260.pdf	CC
VU#144389 - TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding	CE
Fix for handling of static RSA padding failures by dgarske · Pull Request #1229 · wolfSSL/wolfssl · GitHub	CC

CVE Program record	CV
NVD vulnerability detail	NV
No vendor comments have been submitted for this CVE.	
Legacy QID Mappings	
591344 Siemens SCALANCE W1750D Cryptographic issues Vulnerability (SSA-464260, ICSA-18-282-02)	

© [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](#).

Free CVE JSON API [cve.report/api](#)

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