TLS - ROBOT VULNERABILITY FALSE-POSITIVES

PUBLISHED: JULY 29, 2018 | LAST UPDATE: JULY 29, 2018

SUMMARY

In December 2017, CERT Coordination Center (CERT/CC) released Vulnerability Note VU#144389 [1] to report potential new TLS exposures for a variety of vendors to a variant of Hanno Böck's Bleichenbacher Oracle vulnerability. This vulnerability is referred to as ROBOT (Return Of Bleichenbacher's Oracle Threat) [2].

A10 Networks products and ACOS are not affected by the TLS ROBOT vulnerability. However, some vulnerability scanning and detection tools, including the Proof-of-Concept (PoC) robot-detect script [3], may generate false positive reports for TLS ROBOT when tested against certain ACOS systems.

This false-positive is due to a behavior of ACOS for systems, with 3rd-generation SSL/TLS hardware solutions, being misinterpreted by these tools as a valid detection of the vulnerability. A10 Networks addresses such false reports as described in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2017-0009	CVSS 3.0	0.0 Low	TLS: ROBOT False Positive Reports

(a) A10 Networks assigned identifier.

AFFECTED RELEASES

The table below indicates releases of ACOS potentially affected by these false-positives and ACOS releases that address them. ACOS release families not indicated below are not prone to such reports.

Customers using affected ACOS releases can overcome such false reports by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
4.1.4	–	4.1.4-P1	4.1.4-P2
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P8	4.1.1-P9

WORKAROUNDS AND MITIGATIONS

None

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
A10-2017-0009	TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding and may therefore be vulnerable to Bleichenbacher-style attacks. This attack is known as a "ROBOT attack". Impact: A remote, unauthenticated attacker may be able to obtain the TLS pre-master secret (TLS session key) and decrypt TLS traffic. Solution: Disable TLS RSA - affected users and system administrators are encouraged to disable TLS RSA cyphers if possible. Please refer to your product's documentation or contact the vendor's customer service. Apply an update - Some products may have software updates available to address this issue. If an update is available, affected users are encouraged to update product software or firmware. Please see the Affected Vendors list below for more information.

RELATED LINKS

Ref #	General Link
[1]	CERT Coordination Center (CERT/CC), Vulnerability Note VU#144389
[2]	https://robotattack.org/
[3]	https://github.com/robotattackorg/robot-detect

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-27	Initial Publication