ISAKMP-IKE - VPN DISABLED, UDP PORTS OPEN

PUBLISHED: JULY 29, 2018 | LAST UPDATE: NOVEMBER 9, 2018

SUMMARY

Vulnerability scans of the ACOS management interface have shown ISAKMP/IKE (Internet Security Association and Key Management Protocol/Internet Key Exchange) UDP ports to be open when no IKE-based VPNs were configured for A10 Thunder and AX devices.

This behavior does not represent a security risk or exposure in the ACOS system, as received packets on UDP ports 500, 4500, and 4510 will be ignored in such cases. To avoid false reporting of potential ACOS vulnerabilities in this regard, the behavior will be corrected as described further in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	Qualys QID: **42017**	A10	0.0 Low	Remote Access or Management Service Detected

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
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P9	4.1.1-P10
4.1.0	–	4.1.0-P11	4.1.0-P12

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
quaVE-0012	THREAT: A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks. The Results section includes information on the remote access service that was found on the target. Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULTS:
Service name: ISAKMP on UDP port 500.

RELATED LINKS

None

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-29	Initial Publication
2.0	2018-11-09	Updated affected and resolved release information for ACOS 4.1.1 release family.

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.