GUI/AXAPI - VULNERABILITIES #2 - ACOS 3.X, 4.X

PUBLISHED: SEPTEMBER 12, 2018 | LAST UPDATE OCTOBER 11, 2019

SUMMARY

Web application security and vulnerability scans of the ACOS management interface indicated a range of security weaknesses and exposures to potential attacks in the ACOS 3.x and 4.x GUI and AXAPI services. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	[a]	OWASP	Medium	Application Error Disclosure [1]
2	[a]	OWASP	High	Hash Disclosure - MD5 Crypt [2]

[a] No identifier available. See item Summary.

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

Customers using affected ACOS releases can overcome vulnerability exposures 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	–	4.1.1-P4	4.1.1-P5
4.1.1	–	4.1.1-P8	4.1.1-P9
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P11	4.1.0-P12

WORKAROUNDS AND MITIGATIONS

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

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
Application Error Disclosure	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Hash Disclosure - MD5 Crypt	Hash was disclosed by the web server - MD4 / MD5.

RELATED LINKS

None

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-09-12	Initial Publication
2.0	2019-10-11	Added 4.1.100 release family.