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

PUBLISHED: JULY 8, 2019 | LAST UPDATE: OCTOBER 16, 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 4.x GUI and AXAPI services. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	(a)	Acunetix	Medium	Vulnerable Javascript library [1]
2	(a)	Acunetix	Medium	Clickjacking: X-Frame-Options header missing [2]
3	(a)	Acunetix	Medium	Email address found [3]

(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-GR1-P1	4.1.4-GR1-P2
4.1.2	–	4.1.2-P5	4.1.2-P6
4.1.1	–	4.1.1-P10	4.1.1-P11
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P12	4.1.0-P13

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
Vulnerable Javascript library	You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported. Affected items: /gui/static/templates/lib.js

	Details: Detected Javascript library jquery version 2.1.4 from file content.
Clickjacking: X-Frame-Options header missing	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. Affected items: /
Email address found	One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found. Affected items: /gui/static/templates/app/shared/login/management.html Pattern found: app-template@a10networks.com.

RELATED LINKS

Ref #	General Link
[1]	https://www.acunetix.com/vulnerabilities/web/vulnerable-javascript-library/
[2]	https://www.acunetix.com/vulnerabilities/web/clickjacking-x-frame-options-header-missing/
[3]	https://www.acunetix.com/vulnerabilities/web/email-address-found/

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2019-07-08	Initial Publication
2.0	2019-10-11	Added 4.1.100 release chain
2,1	2019-10-16	Corrected resolved release for 4.1.100 release family