GUI - HSTS MISSING IN REDIRECT FROM GET ROOT

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

SUMMARY

A vulnerability scanner reveled an issue related to the ACOS web-GUI management interface that is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	84502	A10	Low	The remote web server is not enforcing HSTS [1]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

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	–	4.1.2-P4	4.1.2-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
3.2.2	–	3.2.2-P5	3.2.2-P6, 3.2.3

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
84502	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. When initially connecting to ACOS Web-GUI via HTTPS, a redirect response to the root page (GET / HTTP/1.1) is missing HTTP Strict Transport Security (HSTS) from the server.

RELATED LINKS

Ref #	General Link
[1]	Nessus 84502

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.