GUI - A10HELP XSS VULNERABILITY

PUBLISHED: AUGUST 9, 2017 | LAST UPDATE: AUGUST 9, 2017

SUMMARY

A vulnerability scan of the ACOS management interface indicated that the Web/GUI access service was potentially exposed to Cross Site Scripting (XSS) attacks for a selected set of help pages. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2017-0006 [a]	A10	n/a	Cross-Site Scripting (XSS) - DOM - a10help

[a] A10 Networks, Inc. assigned identifier.

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
			4.1.2 [a]
4.1.1	–	4.1.1-P1	4.1.1-P2
4.1.0	–	4.1.0-P7	4.1.0-P8
3.1.0-P1	–	3.2.1-P1	3.2.2-P1
			2.8.2, 2.7.2, 2.7.1, 2.6.1-GR1 [a]

[a] Including all updates to the release(s).

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
A10-2017-0006	Summary: The page gui/static/a10help/index.html suffers from a Cross-site Scripting (XSS) vulnerability. Description: Cross-Site Scripting (XSS) is a form of injection attack that occurs when user input is unsafely incorporated into the HTML markup inside of a webpage. When not properly escaped, an attacker can inject malicious JavaScript though it may also include HTML, Flash, or any other type of code that the browser may execute. The malicious script will execute in the browser page DOM of a user typically without their knowledge or consent. Steps to reproduce: 1. Navigate to gui/static/a10help/index.html#t=javascript:alert(document.domain) 2. Observe that XSS executes. In chrome, observe a popup indicating "An embedded page on this webpage says domain.name.of.device/DUT"

RELATED LINKS

None

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-09	Initial Publication