TLS/SSL - DES AND IDEA CIPHERS SUPPORTED

PUBLISHED: JULY 31, 2017 | LAST UPDATE: JULY 31, 2017

SUMMARY

A vulnerability scan of the ACOS management interface indicated that the HTTPS service supported TLS sessions using ciphers based on DES and IDEA algorithms which are no longer recommended for use with TLS 1.2. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	ssl-des-ciphers	Rapid7	6 Severe	TLS/SSL Server Supports DES and IDEA Cipher Suites [1]

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, 4.1.1 [(a)]
4.1.0	–	4.1.0-P7	4.1.0-P8
3.1.0-P1	–	3.1.4	3.1.4-P1
3.2.0	–	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
ssl-des-ciphers	Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on the DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm) algorithms. DES and IDEA algorithms are no longer recommended for general use in TLS, and have been removed from TLS version 1.2.

RELATED LINKS

Ref #	General Link
[1]	Rapid7: TLS/SSL Server Supports DES and IDEA Cipher Suites

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-07-31	Initial Publication