TLS/SSL - CVE-2016-10213

PUBLISHED: JULY 12, 2018 | LAST UPDATE: JULY 12, 2018

SUMMARY

On June 10, 2016, A10 published a blog post entitled *CVE-2016-0270 GCM nonce vulnerability* [1] discussing an issue with how certain devices generate the nonce for AES-GCM. With resolution for CVE identifier assignment complications at the time for CVE-2016-0270 [2], this issue was addressed for the following vulnerabilities and as described further in this document.

Item		**Score**		
#	**Vulnerability ID**	**Source**	**Score**	**Summary**
1	CVE-2016-10213	CVSS 3.0	5.9 Med	AES-GCM Nonce Vulnerability [3]

It was determined that the TLS/SSL data-plane in certain A10 ACOS release families were potentially exposed to exploit due to use randomly generated, AES GCM Nonce values.

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 potentially exposed releases can update ACOS to the indicated resolved release or subsequent updates. If the table does not list a corresponding resolved or unaffected release, then no release update is currently available or anticipated.

Releases Affected			**Releases Resolved or Unaffected**
4.1.0	–	4.1.0-P1	4.1.0-P2
4.0.0	–	4.0.3-P1	4.0.3-P2
2.7.2	–	2.7.2-P7	2.7.2-P8

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**
CVE-2016-10213	A10 AX1030 and possibly other devices with software before 2.7.2-P8 uses random GCM nonce generations, which makes it easier for remote attackers to obtain the authentication key and spoof data by leveraging a reused nonce in a session and a "forbidden attack," a similar issue to CVE-2016-0270.

RELATED LINKS

Ref #	General Link
[1]	A10 Blog - CVE-2016-0270 GCM nonce vulnerability
[2]	NIST NVD, CVE-2016-0270
[3]	NIST NVD, CVE-2016-10213
[4]	Nonce-Disrespecting Adversaries: Practical

ACKNOWLEDGEMENTS

A10 would like to thank Hanno Böck who had discovered issues with how devices generate the nonce for AES-GCM and subsequently published a paper, *Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS* [4], on the topic.

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-12	Initial Publication

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.