Security Advisory

TLS-SSL - CVE-2016-6306

PUBLISHED: JULY 30, 2018 | LAST UPDATE: JULY 30, 2018

SUMMARY

In September 2016, openssl.org released a security advisory detailing several security issues. The following vulnerabilities that may affect the TLS/SSL data plane of ACOS devices reported in that advisory are addressed in this document.

Item		Score		
#	**Vulnerability ID**	**Source**	**Score**	**Summary**
1	CVE-2016-6306	CVSS 3.0	5.9 Med	Certificate message OOB reads

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**
4.1.2	–	4.1.2-P3	4.1.2-P4
4.1.1	–	4.1.1-P8	4.1.1-P9
4.1.0	–	4.1.0-P11	4.1.0-P12
2.7.2	–	2.7.2-P12	2.7.2-P13
2.7.1-GR1	–	2.7.1-GR1-Px	2.7.2-P13, 4.1.0-P12, 4.1.1-P9, 4.1.4
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.2-P13, 4.1.0-P12, 4.1.1-P9, 4.1.4

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-2016-6306	In OpenSSL 1.0.2 and earlier some missing message length checks can result in OOB reads of up to 2 bytes beyond an allocated buffer. There is a theoretical DoS risk but this has not been observed in practice on common platforms. The messages affected are client certificate, client certificate request and server certificate. As a result the attack can only be performed against a client or a server which enables client authentication.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2016-6306

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-30	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.