TLS-SSL - CVE-2016-2182

PUBLISHED: AUG 9, 2018 | LAST UPDATE: AUG 9, 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 #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2016-2182	CVSS 3.0	9.8 Critical	OOB write in BN_bn2dec()

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
4.1.0	–	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-P2
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.2-P13, 4.1.0-P12, 4.1.1-P9, 4.1.4-P2

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-2016-2182	"The function BN_bn2dec() does not check the return value of BN_div_word(). This can cause an OOB write if an application uses this function with an overly large BIGNUM. This could be a problem if an overly large certificate or CRL is printed out from an untrusted source. TLS is not affected because record limits will reject an oversized certificate before it is parsed. OpenSSL 1.0.2 users should upgrade to 1.0.2i OpenSSL 1.0.1 users should upgrade to 1.0.1u

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2016-2182

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-08-09	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.