TLS-SSL - CVE-2018-0739D

PUBLISHED: AUG 9, 2018 | LAST UPDATE: AUG 9, 2018

SUMMARY

In March 2018, 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-2018-0739	CVSS 3.0	6.4 Medium	openssl: Handling of crafted recursive ASN.1 structures can cause a stack overflow and resulting denial of service

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-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2018-0739

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-08-09	Initial Publication