TLS-SSL - CVE-2016-2177

PUBLISHED: OCTOBER 10, 2018 | LAST UPDATE: NOVEMBER 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-2016-2177	CVSS 3.0	9.8 Critical	Pointer arithmetic undefined behaviour

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-P2	4.1.4-P3
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P9	4.1.1-P10
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-P10, 4.1.4-P3
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.2-P13, 4.1.0-P12, 4.1.1-P10, 4.1.4-P3

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-2016-2177	Avoid some undefined pointer arithmetic A common idiom in the codebase is to check limits in the following manner: "p + len > limit" Where "p" points to some malloc'd data of SIZE bytes and limit == p + SIZE "len" here could be from some externally supplied data (e.g. from a TLS message). The rules of C pointer arithmetic are such that "p + len" is only well defined where len <= SIZE. Therefore the above idiom is actually undefined behaviour.

For example this could cause problems if some malloc implementation provides an address for "p" such that "p + len" actually overflows for values of len that are too big and therefore p + len < limit.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2016-2177

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-10-10	Initial Publication
2.0	2018-10-14	Corrected typo in 4.1.4 release chain affected releases.
3.0	2018-11-09	Updated related link to correct CVE entry at NVD.