TLS/SSL - CVE-2016-6304

PUBLISHED: JULY 24, 2017 | LAST UPDATE: JULY 24, 2017

SUMMARY

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

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2016-6304	CVSS 3.0	7.5 High	OCSP Status Request extension unbounded memory growth [1, 2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

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
			4.1.1 [(a)]
4.1.0	–	4.1.0-P5	4.1.0-P6
2.7.2	–	2.7.2-P10	2.7.2-P11
2.7.1-GR1	–	2.7.1-GR1-P1	2.7.2-P11, 4.1.0-P6, 4.1.1 [(a)]
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.2-P11, 4.1.0-P6, 4.1.1 [(a)]

[(a)] Including all updates to the release(s).

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-2016-6304	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.

RELATED LINKS

Ref #	General Link
[1]	OpenSSL Security Advisory [22 Sep 2016]
[2]	NIST NVD, CVE-2016-6304

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-07-24	Initial Publication