TLS-SSL - CVE-2017-3736/3737/3738

PUBLISHED: JULY 22, 2018 | LAST UPDATE: JULY 22, 2018

SUMMARY

In November 2017, December 2017, and March 2018, openssl.org released security advisories detailing several security issues. The following vulnerabilities that may affect the TLS/SSL management and/or data-plane of ACOS devices reported in these advisories are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2017-3736 (a, b)	CVSS 3.0	6.5 Med	openssl: bn_sqrx8x_internal carry bug on x86_64 [1, 4]
2	CVE-2017-3737 (a)	CVSS 3.0	5.9 Med	SSL_read() or SSL_write() error state mechanism [2, 5]
3	CVE-2017-3738 (a, b)	CVSS 3.0	5.9 Med	rsaz_1024_mul_avx2 overflow bug on x86_64 [3, 5, 6]

(a) Affects ACOS Management Plane

(b) Affects ACOS Data Plane.

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

WORKAROUNDS AND MITIGATIONS

MANAGEMENT PLANE

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

DATA PLANE

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-2017-3736	If an X.509 certificate has a malformed IPAddressFamily extension, OpenSSL could do a one-byte buffer overread. The most likely result would be an erroneous display of the certificate in text format. As this is a low severity fix, no release is being made. The fix can be found in the source repository (1.0.2, 1.1.0, and master branches); see https://github.com/openssl/openssl/pull/4276. This bug has been present since 2006.
CVE-2017-3737	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/ SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error.
CVE-2017-3738	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2017-3736
[2]	NIST NVD, CVE-2017-3737
[3]	NIST NVD, CVE-2017-3738
[4]	OpenSSL Security Advisory [02 Nov 2017]
[5]	OpenSSL Security Advisory [07 Dec 2017]
[6]	OpenSSL Security Advisory [27 Mar 2018]

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-22	Initial Publication