TLS-SSL - CVE-2017-3732, CVE-2016-7055

PUBLISHED: JULY 18, 2018 | LAST UPDATE: JULY 18, 2018

SUMMARY

In January 2017, 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-2017-3732	CVSS 3.0	5.9 Med	BN_mod_exp may produce incorrect results on x86_64 [1]
2	CVE-2016-7055	CVSS 3.0	5.9 Med	Montgomery multiplication may produce incorrect results [2]

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
4.1.2	–	4.1.2-P3	4.1.2-P4
4.1.1	–	4.1.1-P7	4.1.1-P8

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-2017-3732	There is a carry propagating bug in the x86_64 Montgomery squaring procedure. 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 DH are considered just feasible (although very difficult) 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 very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. UPDATE 31 Jan 2017. The original text said For example this can occur by default in OpenSSL DHE based SSL/TLS ciphersuites. This is not true. DHE key re-use was removed by commit c5b831f for 1.0.2 or commit ffaef3f for 1.1.0 on 17 December 2015 Note: This issue is very similar to CVE-2015-3193 but must be treated as a separate problem.
CVE-2016-7055	From https://www.openssl.org/news/secadv/20170126.txt [3]: This issue was previously fixed in 1.1.0c and covered in security advisory https://www.openssl.org/news/secadv/20161110.txt OpenSSL 1.0.2 users should upgrade to 1.0.2k From https://www.openssl.org/news/secadv/20161110.txt [2, 4]: There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible. This is because the subroutine in question is not used in operations with the private key itself and an input of the attacker's direct choice. Otherwise the bug can manifest itself as transient authentication and key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input. Among EC algorithms only Brainpool P-512 curves are affected and one presumably can attack ECDH key negotiation. Impact was not analyzed in detail, because pre-requisites for attack are considered unlikely. Namely multiple clients have to choose the curve in question and the server has to share the private key among them, neither of which is default behaviour. Even then only clients that chose the curve will be affected. OpenSSL 1.1.0 users should upgrade to 1.1.0c This issue does not affect OpenSSL versions prior to 1.0.2. Due to the low severity of this defect we are not issuing a new 1.0.2 release at this time. We recommend that 1.0.2 users wait for the next 1.0.2 release for the fix to become available. The fix is also available in the OpenSSL git repository in commit 57c4b9f6a2.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2017-3732
[2]	NIST NVD, CVE-2016-7055
[3]	OpenSSL Security Advisory [26 Jan 2017]
[4]	OpenSSL Security Advisory [10 Nov 2016]

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-18	Initial Publication