TLS-SSL - CVE-2018-0732

PUBLISHED: JULY 22, 2018 | LAST UPDATE: JULY 27, 2018

SUMMARY

In June 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-2018-0732	CVSS 3.0	4.3 Med	openssl: Malicious server can send large prime to client during DH(E) TLS handshake causing the client to hang

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

WORKAROUNDS AND MITIGATIONS

Exposure to this vulnerability can be fully mitigated by disabling DHE-based ciphers in configured ACOS ssl-server templates.

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-2018-0732	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 or 1.0.2 at this time. The fix will be included in OpenSSL 1.1.0i and OpenSSL 1.0.2p when they become available. The fix is also available in commit ea7abeeab (for 1.1.0) and commit 3984ef0b7 (for 1.0.2) in the OpenSSL git repository.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2018-0732

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-22	Initial Publication
2.0	2018-07-27	Added mitigation