TLS-SSL - CVE-2016-2107

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

SUMMARY

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

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2016-2107	CVSS 3.0	5.9 Med	openssl: Padding oracle in AES-NI CBC MAC check [2]
2	91572	Nessus	2.6 Low	OpenSSL AES-NI Padding Oracle MitM Information Disclosure [1]

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
4.1.0	–	4.1.0-P8	4.1.0-P9
3.1.0-P1	–	3.2.1-P1	3.2.2-P1
2.8.2-P10	–	2.8.2-Px	4.1.2, 4.1.4
2.7.2-P11	–	2.7.2-Px	4.1.0-P9, 4.1.1, 4.1.4

WORKAROUNDS AND MITIGATIONS

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.

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-2016-2107	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.

91572	The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256. The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic. Reference: CVE-2016-2107 Evidence: Plugin Output: Nessus was able to trigger a RECORD_OVERFLOW alert in the remote service by sending a crafted SSL "Finished" message.

RELATED LINKS

Ref #	General Link
[1]	Nessus: OpenSSL AES-NI Padding Oracle MitM Information Disclosure
[2]	NIST NVD, CVE-2016-2107

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-22	Initial Publication