TLS/SSL - 3DES CIPHER SUPPORTED, CVE-2016-2183

PUBLISHED: AUGUST 2, 2017 | LAST UPDATE: OCTOBER 21, 2019

SUMMARY

A vulnerability scan of the ACOS management interface indicated that the HTTPS service supported TLS sessions using ciphers based on the 3DES algorithm which is no longer considered capable of providing a sufficient level of security in SSL/TLS sessions. CVE-2016-2183 is a commonly referenced CVEs for this issue. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	ssl-3des-ciphers	Rapid7	1 Moderate	TLS/SSL Server Supports 3DES Cipher Suite [1]
2	CVE-2016-2183	CVSS 3.0	5.3 Medium	SWEET32 Mitigation - OpenSSL [2]
3	ssl-cve-2016-2183-sweet32	Rapid7	5 Severe	TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) [3]
4	42873	Nessus	Medium	SSL Medium Strength Cipher Suites Supported (SWEET32) [4]

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
			4.1.2 (a)
4.1.1	–	4.1.1-P1	4.1.1-P2
4.1.100	–	4.1.100-P5-SP1	4.1.100-P6
4.1.0	–	4.1.0-P7	4.1.0-P8
3.1.0-P1	–	3.1.4	3.1.4-P1
3.2.0	–	3.2.1-P1	3.2.2-P1
2.8.2	–	2.8.2-P9	2.8.2-P10 (b), 4.1.2 (a, c)
2.7.2	–	2.7.2-P10	2.7.2-P11 (b), 4.1.0-P8 (c), 4.1.1-P2 (c)
2.7.1-GR1	–	2.7.1-GR1-P1	2.7.2-P11 (b), 4.1.0-P8 (c), 4.1.1-P2 (c)
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.2-P11 (b), 4.1.0-P8 (c), 4.1.1-P2 (c)

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

(b) Partial Remediation. Expanded cipher suite supported, including 3DES cipher.

(c) Full Remediation. Expanded cipher suite supported, excluding 3DES cipher.

With the 2.7.2 and 2.8.2 resolved releases, the ACOS HTTPS management service additionally supports ciphers that include RSA, ECDHE-RSA, ECDHE-ECDSA, AES, and AES-GCM capabilities. These releases continue to support the 3DES cipher to avoid impacting existing deployment environments with management applications dependent on this cipher.

To fully overcome vulnerability exposures due to the 3DES cipher, the ACOS 4.1 resolved or unaffected releases are available for upgrade.

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
ssl-3des-ciphers	Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on the 3DES (Triple Data Encryption Standard) algorithm. Since 3DES only provides an effective security of 112 bits, it is considered close to end of life by some agencies. Consequently, the 3DES algorithm is not included in the specifications for TLS version 1.3. ECRYPT II (from 2012) recommends for generic application independent long-term protection at least 128 bits security. The same recommendation has also been reported by BSI Germany (from 2015) and ANSSI France (from 2014), 128 bit is the recommended symmetric size and should be mandatory after 2020. While NIST (from 2012) still considers 3DES being appropriate to use until the end of 2030.
CVE-2016-2183	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
ssl-cve-2016-2183-sweet32	Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of the SSL/TLS protocols that support cipher suites which use 3DES as the symmetric encryption cipher are affected. The security of a block cipher is often reduced to the key size k: the best attack should be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an important security parameter, defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than 2 to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.
42873	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. See also : https://www.openssl.org/blog/blog/2016/08/24/sweet32/

RELATED LINKS

Ref #	General Link
[1]	Rapid7: TLS/SSL Server Supports 3DES Cipher Algorithms
[2]	NIST NVD, CVE-2016-2183
[3]	Rapid7: TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)
[4]	NIST CSRC - Update to Current Use and Deprecation of TDEA
[5]	SSL Medium Strength Cipher Suites Supported (SWEET32)

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-02	Initial Publication
2.0	2018-03-07	Update release information for ACOS 2.8.2 and 4.1.1 release families.
3.0	2019-04-18	Added Rapid7 ssl-cve-2016-2183-sweet32 to scope of advisory. Corrected NIST CSRC link.
4.0	2019-10-17	Added 4.1.100 release family.
5.0	2019-10-21	Added Nessus ID 42873.