TLS/SSL - TLS 1.0 PROTOCOL SUPPORTED, CVE-2011-3389

PUBLISHED: AUGUST 3, 2017 | LAST UPDATE: OCTOBER 24, 2019

SUMMARY

Vulnerability scans of the ACOS management interface indicate that the HTTPS service support TLS sessions using TLS 1.0 protocol which is no longer considered capable of providing a sufficient level of security TLS sessions or complying with contemporary PCI (Payment Card Industry) security standards [3]. CVE-2011-3389 (aka BEAST attack) is a commonly referenced CVEs for this issue as the commonplace mitigation for this vulnerability is to disable TLS 1.0 support. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	tlsv1_0-enabled	Rapid7	4 Severe	TLS Server Supports TLS version 1.0 [1]
2	QID: 38628	Qualys	3 Serious	SSL/TLS Server supports TLSv1.0 [2]
3	CVE-2011-3389	CVSS 2.0	4.3 Medium	HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST) [4]
4	ssl-cve-2011-3389-beast	Rapid7	4 Severe	TLS/SSL Server is enabling the BEAST attack [5]
5	58751	Nessus	Medium	SSL/TLS Protocol Init Vector Implem Infor Disclosure Vuln (BEAST) [6]

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
4.1.0	–	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. TLS 1.0, 1.1, and 1.2 are supported.

(c) Full Remediation. TLS 1.2 only is supported.

With the 2.7.2 and 2.8.2 resolved releases, the ACOS HTTPS management service additionally supports TLS 1.1 and 1.2 protocols. These releases continue to support the TLS 1.0 protocol to avoid impacting existing deployment environments with management applications dependent on this cipher.

To fully overcome vulnerability exposures associated with the TLS 1.0 protocol, 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
tlsv1_0-enabled	The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2.
QID: 38628	TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode. RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security. A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade. This QID will be marked as a Fail for PCI as of November 1st, 2016 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018. Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1 (https://community.qualys.com/message/34120).
CVE-2011-3389	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
ssl-cve-2011-3389-beast	The SSL protocol, as used in certain configurations of Microsoft Windows and browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (and other products negotiating SSL connections) encrypts data by using CBC mode with chained initialization vectors. This potentially allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. By supporting the affected protocols and ciphers, the server is enabling the clients in to being exploited.
58751	A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system. TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected. This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable. OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

RELATED LINKS

Ref #	General Link
[1]	Rapid7: TLS Server Supports TLS version 1.0
[2]	QID 38628 - Server Supports TLS 1 Severity 3
[3]	PCI Security Standards Council - Information Supplement - Migrating from SSL and Early TLS
[4]	NIST NVD, CVE-2011-3389
[5]	Rapid7: TLS/SSL Server is enabling the BEAST attack
[6]	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-03	Initial Publication
2.0	2018-03-07	Update release information for ACOS 2.8.2 and 4.1.1 release families. Corrected release information for ACOS 4.1.0.
3.0	2019-04-18	Added Rapid7 ssl-cve-2011-3389-beast to scope of advisory.
4.0	2019-10-17	Added 4.1.100 release family.
5.0	2019-10-21	Added Nessus ID 58751.
6.0	2019-10-24	Removed 4.1.100 release family, not exposed.