TLS/SSL - RC4 CIPHERS SUPPORTED, CVE-2013-2566, CVE-2015-2808

PUBLISHED: AUGUST 1, 2017 | LAST UPDATE: AUGUST 1, 2017

SUMMARY

A vulnerability scan of the ACOS management interface indicated that the HTTPS service supported TLS sessions using ciphers based on the RC4 algorithm which is no longer considered capable of providing a sufficient level of security in SSL/TLS sessions. CVE-2013-2566 and CVE-2015-2808 are commonly referenced CVEs for this issue. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	rc4-cve-2013-2566	Rapid7	4 Severe	TLS/SSL Server Supports RC4 Cipher Algorithms [1]
2	CVE-2013-2566	CVSS 3.0	5.9 Medium	SSL/TLS: Attack against RC4 stream cipher [2]
3	CVE-2015-2808	CVSS 2.0	4.3 Medium	SSL/TLS: "Invariance Weakness" vulnerability in RC4 stream cipher [3]

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, 4.1.1 [(a)]
4.1.0	–	4.1.0-P7	4.1.0-P8
			3.1.x, 3.2.x [(a)]
			2.8.2, 2.7.2, 2.7.1, 2.6.1-GR1 [(a)]

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

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
rc4-cve-2013-2566	Recent cryptanalysis results exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts. As a result, RC4 can no longer be seen as providing a sufficient level of security for SSL/TLS sessions. It has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.
CVE-2013-2566	The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.
CVE-2015-2808	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.

RELATED LINKS

Ref #	General Link
[1]	Rapid7: TLS/SSL Server Supports RC4 Cipher Algorithms
[2]	NIST NVD, CVE-2013-2566
[3]	NIST NVD, CVE-2015-2808

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-01	Initial Publication