SECURITY ADVISORY

#CVE-2015-7575 published on January 6th, 2016

Summary Description

This security advisory addresses CVE-2015-7575, pertaining to TLS1.2 in non FIPS compliant versions of ACOS.

Details

TLS 1.2 allows for the client and server to negotiate the hash algorithm they use. This was designed to allow the use of stronger hash functions, however it does allow for the use of the weaker MD5, which effectively weakens the authentication.

In the FIPS compliant versions of ACOS, this hash is specifically disabled; however the rest of the code is affected.

Although unlikely to exploit, if the vulnerability is exploited it can give the attacker one of two advantages. They may be able to forge a client certificate thus thwart certificate based client authentication. The second vulnerability would allow for key to be forged while using the server-key-exchange option.

This vulnerability requires the attacker is positioned on the network in a way allowing for the intercept of traffic and is very complex and difficult to exploit.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *4.0.1, 3.x, 2.7.2-P7, 2.7.1-GR1, 2.8.2-P4*

Software Updates

Software updates resolving this potential vulnerability will be published at the following URL when available:

http://www.a10networks.com/support-axseries/downloads/downloads.php

The following table summarizes update versions resolving all of the above CVEs.

Vulnerable Release	Resolved Release
4.0.1	4.1.0
3.x	3.2.1
2.7.2-P7	2.7.2-P8
2.7.1-GR1	2.7.1-GR1-P1
2.8.2-P4	2.8.2-P5

References

1. NIST-NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7575
2. MITRE-DB, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7575
3. RedHat, https://access.redhat.com/security/cve/cve-2015-7575