SECURITY ADVISORY

#CVE-2015-3195 published on December 3rd, 2015

Summary Description

On December 3rd, 2015, OpenSSL release a security advisory[1] with a number of security vulnerabilities across multiple version of OpenSSL. Out of those ACOS is only affected by CVE-2015-3195[2] and this advisory addresses the impact from it.

Details

If a specially crafted certificate is uploaded to ACOS device it is theoretically possible to trigger a bug in the way X.509 date is handled, which may result in a memory leak.

In order to upload certificates to the device the user already needs to have higher level of privilege which overall implies they would have access to the data leaked regardless of the use of this bug.

Mitigation Recommendations

None.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *4.0.x, 3.1.x, 2.7.x, 2.8.X*

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

Since this is a minor vulnerability, the patch will be included in the next scheduled software release.

References

1. OpenSSL Security Advisory – 2015-12-03: https://www.openssl.org/news/secadv/20151203.txt
2. NIST-NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3195