SECURITY ADVISORY

#CVE-2016-2108 published on May 5th, 2016

Summary Description

On May 3rd, the OpenSSL published a security advisory detailing a number of vulnerabilities in OpenSSL mostly related to input validation. At least two of them, if aligned properly can lead to third party controlled code execution.

Details

Some versions of ACOS include vulnerable version the OpenSSL library. The vulnerabilities affecting it and which are addressed by this software update are: CVE-2016-2108, CVE-2016-2105, CVE-2016-2106, CVE-2016-2109 and CVE-2016-2176).

The most notable is CVE-2016-2108 which is ranked "high severity" and could potentially expose the device to an underflow and crash, when verifying and re-encoding certificates.

Mitigation Recommendations

Currently there is no way to mitigate the impact of those.

Vulnerability Assessment

Affected Platforms: *ADC, CGN*

Affected Software Versions: *4.0.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

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

Vulnerable Release	Resolved Release
4.0.3-P1	4.0.3-P2
4.1.0-P1	4.1.0-P2
	4.1.1
2.7.2-P7	2.7.2-P7-SP8
2.7.2-P7	2.7.2-P8
2.7.1.GR1-P1	2.7.1-GR1-P2

References

1. OpenSSL Security Advisory – 2016-05-03: https://openssl.org/news/secadv/20160503.txt
2. NIST-NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2108
3. MITRE-DB, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2108