SECURITY ADVISORY

#CVE-2014-3571, 3569, 3572, 8275, 3570 and #CVE-2015-0204, 0205, 0206, published before[1] and on January 8th, 2015

Summary Description

On January 8th, 2015, the OpenSSL Project announced a patch release addressing a number of low-level and a couple of moderate-level vulnerabilities. The patches cover the following CVEs:

- CVE-2014-3571 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3571)
- CVE-2015-0206 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0206)
- CVE-2014-3569 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3569)
- CVE-2014-3572 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3572)
- CVE-2015-0204 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204)
- CVE-2015-0205 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0205)
- CVE-2014-8275 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8275)
- CVE-2014-3570 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3570)

This document is a combined response of A10 Networks to the aforementioned vulnerabilities.

Despite the fact that CVE-2014-3571 and CVE-2015-0206 are rated with "moderate" level of severity by the Open SSL project, they do not appear to be an issue for A10 appliances and software. Both of those vulnerabilities affect DTLS and currently A10 does not have any software using it.

The following CVEs are low severity, do not pose an immediate threat to the devices and will be resolved in the next regular software release:

- CVE-2014-3569
- CVE-2014-3572
- CVE-2015-0204
- CVE-2014-8275
- CVE-2014-3570

[1] CVE-2014-3569, CVE-2014-0204 and CVE-2014-0205 were originally published on 12/24/2014, 11/03/2014 and 09/28/2014 respectively

CVE-2015-0205 is not an issue for ACOS since at present the software does not support certificate authentication.

Vulnerability Assessment

Affected Platforms: *ADC*

Affected Software Versions: *ADC 2.6/2.7/4.0, TPS 3.0.0*

Mitigation Recommendations

A10 Networks recommends upgrading to the respective patches when available. The table below summarizes the software releases resolving that issue.

Vulnerable Release	Resolved Release
2.6.1-GR1-P14	2.6.1-GR1-P15
2.7.0-P6	2.7.0-P7
2.7.1-P6	2.7.1-GR1
2.7.2-P4	2.7.2-P5
3.0.0	3.1.1
4.0.0	4.0.1