SECURITY ADVISORY

#CVE-2015-{1788, 1789, 1790, 1791 and 1792} published on June 11th, 2015

Summary Description

This security advisory addresses a number of vulnerabilities in OpenSSL that were released on June 11th, 2015.

Details as Pertaining to A10 Software and Equipment

A10 device can both be a server and a client in SSL/TLS connection. The exploitation can occur when a device is processing specially crafted certificate supplied by the other side.

If the A10 device is a client it can be exploited by a server, and if the A10 device is the server it can potentially be exploited by a client if client certificate authentication is enabled.

CVE-2015-1788 – Malformed ECParameters causes infinite loop
Successful exploitation of this vulnerability would lead an infinite loop which will lead to a denial of service, however no remote code execution is possible.

CVE-2015-1789 – Exploitable out-of-bounds read in X509_cmp_time
This vulnerability is caused by a couple of failures in the X509_cmp_time function, which can be triggered by a malformed time format in certificate.

Successful exploitation of this vulnerability would lead to segmentation fault and thus a denial of service condition. Currently we do not possess any information that this can be exploited to gain control of the device and due to the very little space available it is unlikely that this is possible. OpenSSL is also classifying this as a DoS condition but not remotely exploitable to execute code.

CVE-2015-1790 - PKCS7 crash with missing EnvelopedContent

PKCS#7 parse code doesn't handle missing inner EncryptedContent correctly, which will trigger a NULL pointer deference.

CVE-2015-1792 - CMS verify infinite loop with unknown hash function
A10 does not support CMS and the affected code is not included in our build.

CVE-2015-1791 - Race condition handling NewSessionTicket
A10 offers very limited ticket support and the code affected is not included in our build.

CVE-2014-8176 – Invalid free in DTLS
A10 does not support DTLS.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *2.6.1-GR1-X, 2.7.X, TPS 3.x.x, 4.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
3.0	3.0-P2-SP22
3.1.2	3.1.3
3.1.x	3.1.3
2.6.1-GR1-P14	2.6.1-GR1-P15
2.7.0-P6	2.7.0-P7
2.7.1-GR1	2.7.1-GR1-P1
2.7.2-P4	2.7.2-P5
4.0.1	4.0.2

References

1. OpenSSL Security Advisory – 2015-03-08: https://www.openssl.org/news/secadv_20150611.txt