SECURITY ADVISORY

#CVE-2014-8730 published on December 8th, 2014

Summary Description

Early in November, A10 Networks was notified of an issue with its implementation of TLS, which allows a padding oracle attack to be executed against it. The issue is in the way the protocol is implemented and that there is no proper padding checking in compliance with RFC 5246. This effectively introduces vulnerability similar to the one in SSLv3, where the padding is not defined as a part of the protocol specification - which opened CBC ciphers in SSLv3 to exploitation.

The vulnerability is assigned CVE-2014-8730 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8730).

In general, this bug can be exploited remotely - allowing an attacker to decrypt sensitive data in the SSL connection. At this point, there is no work around and it is necessary to apply the patches provided below.

Vulnerability Assessment

Affected Platforms: *ADC*

Affected Software Versions: *2.6.1-GR1, 2.7.x*

Mitigation Recommendations

A10 Networks recommends upgrading to the latest available patch release:

Technology	Major Release	Fixed	Latest Patch
ADC	2.6.1-GR1	2.6.1-GR1-P13-SP3	2.6.1-GR1-P13
ADC	2.7.0-P6	2.7.0-P6-SP4	2.7.0-P6
ADC	2.7.1-P5	2.7.1-P5-SP10	2.7.1-P5
ADC	2.7.2-P3	2.7.2-P3-SP5	2.7.2-P3

Software Updates

Patches for the CVE-2014-3566 Poodle/SSL v3.0 vulnerability are here:
http://www.a10networks.com/support-axseries/downloads/downloads.php#CVE-2014-3566