Entuity Software Notification

Technical Bulletin

Version 2014.10.27
October 27, 2014

SSL 3.0 “POODLE” Vulnerability Notification Correction

It has come to our attention that Technical Bulletin “Version 2014.10.20” contained inaccuracies in the procedure for eliminating the SSL 3.0 “POODLE” (Padding Oracle On Downgraded Legacy Encryption) security vulnerability. The purpose of this notification is to provide the required fix to eliminate the vulnerability.

In order to eliminate this security vulnerability from your Entuity installation, SSLv3 can be disabled using the following procedure:

- For Entuity 14 and above:
  - Modify the following Apache configuration files:

    <*Entuity Home*>\install\template\lib\apache\conf\httpd_eye.conf
    From: ##CONFIGPARSE## SSLProtocol -ALL +SSLv3 +TLSv1
    To: ##CONFIGPARSE## SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2

    <*Entuity Home*>\lib\apache\conf\httpd_eye.conf
    From: SSLProtocol -ALL +SSLv3 +TLSv1
    To: SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2

  - Then restart Entuity Web Server:
    <*Entuity Home*>*bin**stop webserver*

    The Web Server will automatically restart after stopping.

  Please note the following differences from the instructions in Technical Bulletin 2014.10.20:
  - +TLSv1 replaces +TLSv1.0.
  - -ALL replaces –ALL (hyphen character in place of en dash character).
  - Restart of Web Server only. Full restart of Entuity installation is not required.

- For all versions below Entuity 14, please contact Entuity for further advice.

We apologize for any inconvenience that may have been caused from instructions provided in the previous notification.