Entuity Software Notification

Technical Bulletin

Version 2014.10.20
October 20, 2014

SSL 3.0 “POODLE” Vulnerability

A major security vulnerability has been discovered on servers that run SSL 3.0. The vulnerability has been named “POODLE” (Padding Oracle On Downgraded Legacy Encryption) and affects all versions of Entuity. The purpose of this notification is to explain how Entuity software is exposed to this vulnerability and to provide a fix to eliminate the vulnerability.

This vulnerability affects all servers running SSL 3.0. It centers on cipher block chaining (CBC) encryption implementation and allows Man-in-the-Middle (MITM) attacks to derive the contents of a secure payload based on responses received from requests sent from a compromised browser to a legitimate server.

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

- 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 +TLSv1.0 +TLSv1.1 +TLSv1.2

  <*Entuity Home*>\lib\apache\conf\httpd_eye.conf
  From: SSLProtocol -ALL +SSLv3 +TLSv1
  To: SSLProtocol –ALL +TLSv1.0 +TLSv1.1 +TLSv1.2

- Then restart your Entuity installation.