The POODLE OpenSSL Vulnerability and Mail Express

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- Mail Express v3.3 - v4.1.0 (Version 4.1.1 disables the protocol.)

DISCUSSION

The "POODLE Vulnerability" (CVE-2014-3566) is a serious vulnerability in the blueprints of SSL v3.0 and thus affects any product following the protocol. This weakness allows stealing the information protected, under normal conditions, by the SSL encryption used to provide communication security and privacy over the Internet for applications such as web, email, instant messaging (IM), and some virtual private networks (VPNs).

Mail Express supports SSL v3 which is vulnerable, however, work is in progress to update the default configuration to mitigate this vulnerability. Customers can manually change their configuration as described below.

WORKAROUND

Note: Mail Express 4.1.1 disables the SSL protocol v 3.0 for **new** installations. Administrators of existing Mail Express installations need to manually disable the compromised protocol as described below.

Configure the Mail Express web server to disable SSLv3 protocol by editing the **server.xml** file four requires you to restart the server.

1. All <Connector> sections should have:

   SSLProtocol="TLSv1"

   and not:
   SSLProtocol="all"

1. All <Connector> sections should have sslEnabledProtocols populated as:

   sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

1. Locate each <Connector> section and search for the ciphers parameter, and then remove any cipher

   The resulting cipher list should look like this:

   ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WIT
   TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_W

1. Save the file and restart the Mail Express server service. You can verify the changes are in effect
   load).