The POODLE OpenSSL Vulnerability and Enhanced File Transfer (EFT)

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT and EFT Enterprise, v4 - v7.0.3.13 (Version 7.0.3.14 disables the protocol.)

DISCUSSION

The "POODLE Vulnerability" (CVE-2014-3566) is a serious vulnerability in the popular OpenSSL cryptographic software library (through version 1.0.1i). 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).

EFT supports SSL connections for HTTPS and FTPS. For broad client support and backward compatibility, SSLv3 can be enabled on EFT. The SSLv3 protocol is vulnerable to the POODLE exploit. It is highly recommended, therefore, that you verify and modify the SSL configuration of EFT as needed to protect your information assets.

WORKAROUND

Note: EFT version 7.0.3.14 disables the SSL protocol v 3.0 for ***new*** installations. Administrators of existing EFT installations need to manually disable the compromised protocol as described below.

1. Log in to the EFT administration interface, and click the **Server** tab.
2. In the left pane, click the server (topmost) node.
3. In the right pane, click the **Security** tab.
4. Under SSL Compatibility, click **Defined**, and then select *only* the **TLS 1.0** check box. (Clear the **SSL 3.0** and **SSL 2.0** check boxes, if selected.)
5. Ensure that your EFT Administration channel is properly secured:

- ***Disallow remote connections*** to the server if at all possible, and simply RDP into the server computer to perform administration functions against the local system.
- If you do allow remote administration, ensure that you enable SSL and restrict IP addresses to only those computers on your network that need to connect for administration of the server. That is, on the **Administration** tab, change **Server administrator listening IP** from **All Incoming** to one or more specific IP addresses.

The POODLE OpenSSL Vulnerability and Enhanced File Transfer (EFT)

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11187/The-POODLE-OpenSSL-Vulnerabi...