Protecting Against POODLE Attacks

Topics

Overview

POODLE (Padding Oracle On Downgraded Legacy Encryption) is an attack against a design flaw in the SSL 3.0 protocol which allows attackers to decode the encrypted data of a secure SSL 3.0 connection. Refer to http://googleonlinesecurity.blogspot.ca/2014/10/this-poodle-bites-exploiting-ssl-30.html and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 for detailed descriptions.

The POODLE attack allows for a man-in-the-middle to intercept a communication between two systems using SSL 3.0 (e.g. client and server). The man-in-the-middle attack involves Javascript from the attacker running in the user's browser. The Javascript is used to submit the specially formatted requests to the server, reconnecting as needed. The man-in-the-middle causes connection errors forcing a protocol downgrade to SSL 3.0. The man-in-the-middle also is used to manipulate the part of the encrypted data that the attack is trying to decode.

The attack does not allow the attackers to decode entire conversations with a single connection; it takes 256 SSL 3.0 requests to reveal one byte of encrypted information.

Any systems and applications utilizing SSL 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable to the POODLE attack.

The best way to protect against the POODLE attack is to disable SSL 3.0 support completely. If the SSL 3.0 communication link is broken, then the POODLE attack cannot happen. However, Disabling SSL 3.0 may impact connectivity or interoperability between clients and servers.

What Products are Affected?

Customers that have *previously* enabled SSL communication features (see "Enabling SSL Communication" in the associated Administration Guide) and are using one of the listed products below are affected.

- Equitrac Office 5.0, 5.1, 5.2, 5.3 and 5.4
- Equitrac Office 4.2.6 and earlier
- Equitrac Express 5.0, 5.1, 5.2, 5.3 and 5.4
- Equitrac Express 4.2.6 and earlier
- Equitrac Professional 5.0 through 5.6
- Xerox Secure Print Management Suite (XSPMS) 5.3 and 5.4
- Xerox Secure Access (XSA) 5.3
- Xerox Secure Access (XSA) 4.1.1

For customers that have not enabled SSL communications and wish to do so, follow the steps in this guide to disable SSL 3.0 and apply the necessary patches to enable SSL support.

For Equitrac Express, Equitrac Office, XSPMS and **XSA**, disable SSL 3.0 in the following areas:

- Apply a hotfix to correct an issue with the EQEnableSSL tool on 64-bit systems. (see **Applying the EQEnableSSL Hotfix** on page 3)
- In the Windows registry for the following: (see **Disabling SSL 3.0 in Windows Registry** on page 3)
  - Servers running CAS (Scheduler), DRE, DCE (DWS), DME, SPE
  - Workstations running DRC (optional but recommended)
  - Workstations running System Manager (optional but recommended). Important for User Tools and EQCmd
  - Web Client servers
  - Active Directory server
- LDAP servers (see **Disabling SSL 3.0 in LDAP Servers** on page 6)
- DWS (see **Disabling SSL 3.0 with DWS Hotfix** on page 6)
- Force HTTPS protocol in IIS for Web Client (see **Enabling HTTPS for Web Client Servers** on page 7)

For Equitrac Professional, disable SSL 3.0 in the following areas:

- In the Windows registry for the following: (see **Disabling SSL 3.0 in Windows Registry** on page 3)
  - Servers running CAS (Scheduler), CPS, DRE,DCE, DME or SPE
  - Web Client servers
  - Active Directory servers
- LDAP servers (see **Disabling SSL 3.0 in LDAP Servers** on page 6)
- Force HTTPS protocol in IIS for Web Client (see **Enabling HTTPS for Web Client Servers** on page 7)

Steps to Protect Against POODLE Attacks

Applying the EQEnableSSL Hotfix

In order to correct an issue with servers running on 64-bit architectures, apply the following hotfixes. The hotfix does not apply to Equitrac services running on 32-bit architectures.

- Equitrac Office/Express/XSA/XSPMS 5.4 – **EQ54-HF-238665-Tools.msp**
- Equitrac Office/Express/XSA/XSPMS 5.3 – **EQ53-HF-238600-Tools.msp**
- Equitrac Office/Express 4.2.6 – **EO-EE426-HF-238526-Tools.exe**

Customers running Equitrac Office/Express versions 4.x (prior to 4.2.6), must upgrade to 4.2.6 and then apply the patch.

Customers running Equitrac Office/Express/XSA/XSPMS versions 5.0, 5.1, 5.2 must upgrade to 5.3 or 5.4, and then apply the patch.

Customers running Xerox Secure Access 4.1.1 must upgrade to Xerox Secure Access 5.3 and then apply the patch.

The patch must be installed on all Equitrac servers in an installation. Once the patch has been applied, re-run the **EQEnableSSL.exe –e** command (as Administrator) to re-enable SSL support in the product. Refer to "Enabling SSL Communication" in the associated Administration Guide for further details.

The EQEnableSSL.exe tool is located in the following product folders:

- **Program Files\Equitrac\Office\Tools**
- **Program Files\Equitrac\Express\Tools**
- **Program Files\Xerox\Xerox Secure Print Manager Suite\Tools**
- **Program Files\Xerox\Xerox Secure Access\Tools**

Disabling SSL 3.0 in Windows Registry

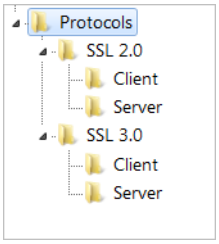
In order to disable SSL 3.0 support for servers and clients, the Windows registry must be edited. Windows Server 2008 supports SSL 2.0, SSL 3.0 and TLS 1.0 protocols, and Windows Server 2008 R2 and Windows 7 support SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2. Although SSL 2.0 is the only security protocol displayed by default in the registry, SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2 are all enabled by default even though the entries are not present in the registry. Refer to the following Microsoft Knowledge Base article for more details (http://support2.microsoft.com/default.aspx?scid=kb;EN-US;245030#top).

To manually edit the Windows registry to disable SSL 3.0, do the following:

1. Select **Start** > **Run**.
2. Type **regedit** and click **OK** to open the Registry Editor.
3. In the Registry Editor, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocol
4. Under **Protocols**, add the **SSL 3.0** key.
5. Within the SSL 3.0 key, add **Client** and **Server** keys.

6 In both of the Client and Server keys, create the following DWORD values:

- **DisabledByDefault** with a value of **1**.
- **Enabled** with a value of **0**.



7 Open the SSL 2.0 key, and set the **Enabled** value to **0** in both the Client and Server keys.

8 Reboot the server.

9 After reboot, test all applications on the Client and Server for compatibility before rolling out the change.

Although the TLS protocols are enabled by default, they do not appear in the registry. After disabling SSL 2.0 and SSL 3.0, it is a good idea to ensure that at least one of the TLS protocols are enabled.

To verify that the TLS protocol is enabled, do the following:

1 Create keys for one or all of the TLS 1.0, TLS 1.1 and TLS 1.2 protocols.

2 Within each of the protocol keys, add **Client** and **Server** keys.

3 Within each of the Client and Server keys, create the following DWORD values:

- **DisabledByDefault** with a value of **0**.
- **Enabled** with a value of **1**.

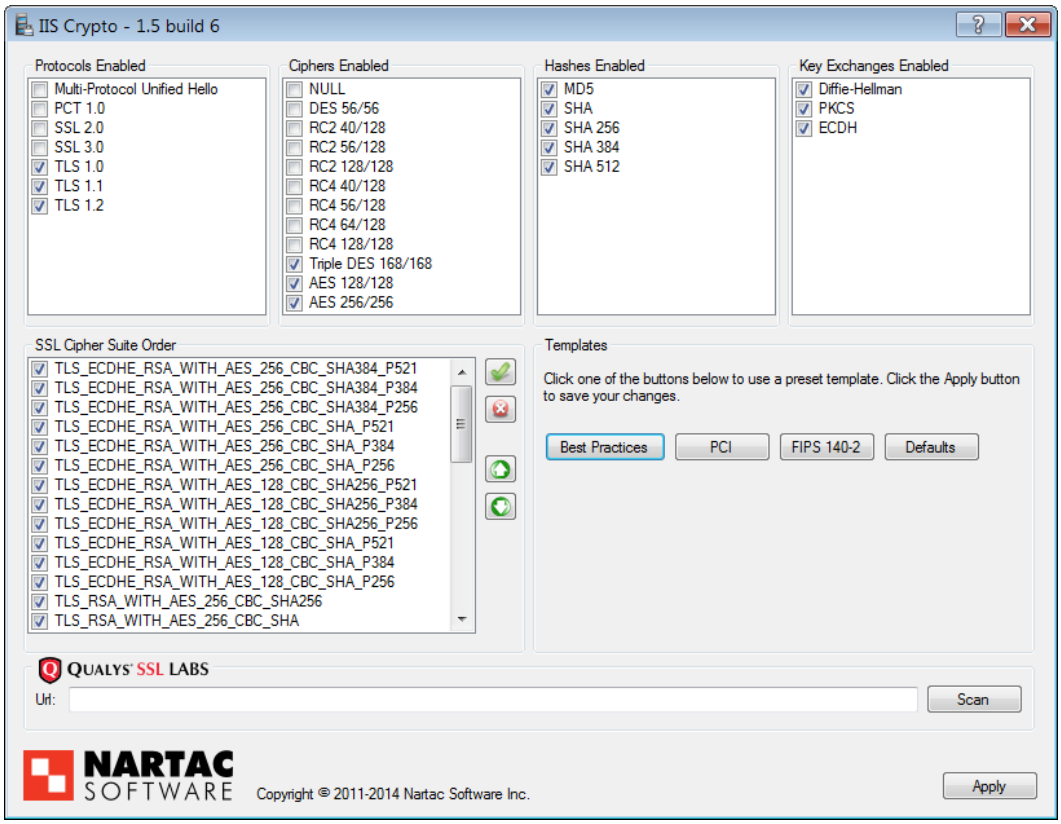
4 Reboot the server if required.

Alternatively, the registry can be modified using a software tool such as IIS Crypto to quickly make changes without manually editing the registry itself.

To use IISCrypto to edit the Windows registry, do the following:

1 Go to https://www.nartac.com/Products/IISCrypto/ and download the appropriate GUI or command line tool.

2 Run the tool to open the UI.



3 Select the desired **Protocols** to enable on the client and server, and deselect the protocols you want to disable.

—Or—

Click **Best Practices** to allow the program to select the most appropriate protocols and ciphers for your system.

4 Click **Apply**.

5 **Reboot** your computer for the changes to take effect. IIS Crypto does not reboot your computer.

6 After reboot, ensure that SSL 3.0 is disabled in the registry.

Disabling SSL 3.0 in LDAP Servers

Some components do not provide configuration parameters to disable SSL 3.0. Currently, the following components fall into this category:

- OpenLDAP
- CUPS

It is possible to disable SSL 3.0 for these components by using stunnel. Stunnel provides an encryption wrapper between a remote client and a local (inetd-startable) or remote server, using the OpenSSL library for cryptography.

To disable SSLv3 on stunnel, use the following configuration parameters in the stunnel.conf file:

```
options = NO_SSLv2

options = NO_SSLv3
```

Installation and configuration of stunnel is outside the scope of this solution. Please consult the man pages and system documentation for more details.

NOTE: Newer openldap-servers have a TLSProtocolMin option. If openldap-servers is openldap-servers-2.4.39-8.el6(for RHEL6), openldap-servers-2.4.39-3.el7(for RHEL7) or later, add "TLSProtocolMin 3.1" in slapd.conf to disable SSL 3.0. You can refer to man slapd.conf.

See https://access.redhat.com/solutions/1234843 for details.

Disabling SSL 3.0 with DWS Hotfix

In order to disable SSL 3.0 for DWS components, apply the following hotfixes (**EQ54-HF-237763-DWS** and **EQ53-HF- 237764-DWS**). The DWS hotfixes support Equitrac Office and Express versions 5.3 and 5.4.

It is sufficient to patch only the client *or* the server with the DWS hotfix in order to prevent POODLE attacks. As long as either the client or the server does not support SSL 3.0, the attack cannot happen. By applying DWS hotfixes, MFPs that are configured for HTTPS communications are protected from POODLE attacks when interacting with Equitrac server products.

When disabling SSL 3.0 from servers hosting MFP web configuration pages, the managed devices must support TLS 1.x in order for the Administrator to manage/update the device, and to maintain secure communication between server and the networked device.

Customers should contact their MFP manufacture/representative to determine if new firmware is available to disable SSL 3.0 from the networked devices, and to determine if any devices within their environment do not support TLS 1.x. Additionally, the MFP representative should provide a list of devices that are vulnerable to the POODLE attack, and provide any available patches.

Additional Security Considerations

Enabling HTTPS for Web Client Servers

In addition to disabling SSL 3.0 on all servers, we recommend that Web Client servers use HTTPS communication for further security. Before enabling HTTPS communication on the Web Client, ensure that Web Client works using standard HTTP communication. For example, it can be accessed through "https://<servername>/WebClient". By default, the Web Client is configured to use port 80 and HTTP binding. For HTTPS communication, the HTTPS binding has to be added to your web site. HTTPS communication requires a certificate.

In order to enable HTTPS communication for Web Client servers, do the following:

- Obtain a Trusted certificate
- Add HTTPS binding
- Force HTTPS protocol

Obtain a Trusted Certificate

For Web Client servers, creating a Domain Certificate through an Enterprise CA is the preferred method. A domain certificate is an internal certificate that does not have to be issued by an external certification authority (CA). If your domain has a server that acts as a CA, you can create a domain certificate and trust that server, and in turn, that trust is passed to all certificates that are signed by that server.

The next best option it to generate a certificate request using the Certificate Wizard, and send the request to a trusted external CA to obtain and import a trusted certificate.

Additionally, you can generate a self-signed certificate in IIS. The disadvantage of a self-signed certificate is that end-users are prompted to accept the certificate the first time they access a Web Client server. There is no such prompt for a trusted certificate.

Add HTTPS Binding

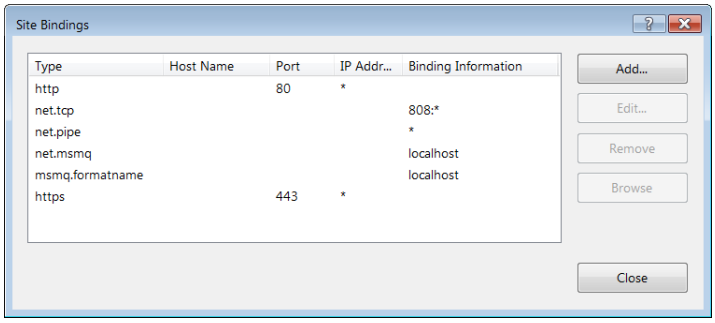
To add HTTPS bindings in IIS, do the following:

1 Open the **Internet Information Services (IIS) Manager**.

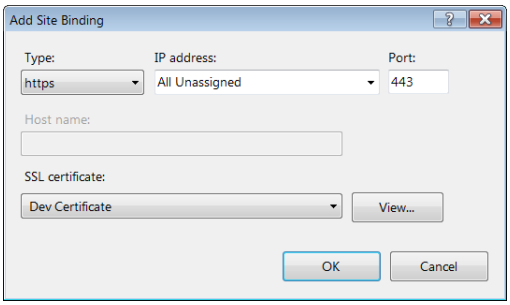
2 In the **Connections** navigation pane, select the web site that contains the **WebClient** web application. In the case of a default installation, this site is the Default Web Site.

3 In the right **Actions** pane, select **Bindings** in the **Edit site** section.

4 In the **Site Bindings** dialog, click the **Add** button.



5 In the **Add Site Binding** dialog, select **https** from the **Type** drop-down list, and select the self-signed certificate from the **SSL certificate** drop-down list, and then click **OK**.



The Web Client is now available through HTTPS communication. For example, it can now be accessed through "https://<servername>/WebClient".

NOTE: When a self-signed certificate is used, a certificate error may be displayed in the browser. Accept the certificate exception to continue.

Force HTTPS Protocol

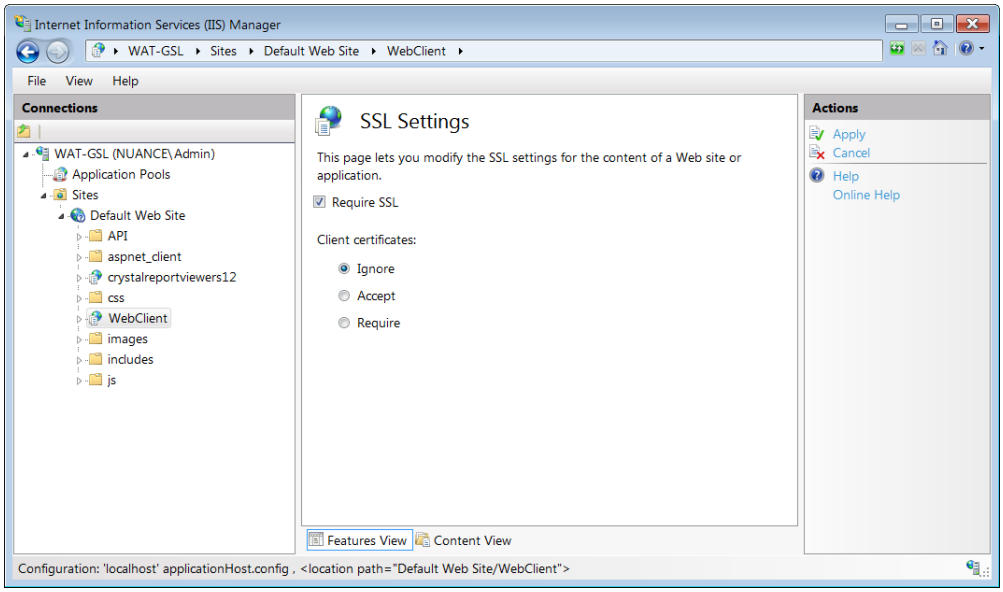
To make the configuration more secure, you can disable the HTTP communication method, so users are forced to use the secure HTTPS protocol.

To force HTTPS protocol and disable HTTP in IIS, do the following:

1 In the **Connections** navigation pane, select the **WebClient** web application.

2 Double-click the **SSL Settings** icon.

3 Select the **Require SSL** checkbox. This option makes IIS reject requests on HTTP.



4 Close IIS Manager.