TMSとOpenSSLベースのデバイス間のTLS問題の原因となるWindowsの暗号

内容

概要

このドキュメントでは、Cisco Telepresence Management Suite(TMS)が管理対象デバイスに接続できず、Cisco TMSで「https応答なし」エラーが報告された場合に発生する問題について説明します。Cisco TMSが会議の開始/管理/監視に失敗する。

背景説明

このソリューションを試す前に、TMSと管理対象デバイス自体の間の接続をトラブルシューティングする必要があります。

次の手順を実行します。

1. TMSサーバでキャプチャソフトウェアを使用します(例：Wireshark)を使用して、TMSと管理対象デバイス間のネットワーク接続を保証します。

2.次のテクニカルノートに従います。

- https://www.cisco.com/c/en/us/support/docs/conferencing/telepresence-management-server/118387-technote-tms-00.html
- https://www.cisco.com/c/en/us/support/docs/conferencing/telepresence-management-suite-tms/211279-How-to-Troubleshoot-No-HTTPS-response.html

問題

パケットキャプチャの分析は、TMSをホストするWindowsサーバと、会議ブリッジやエンドポイントを含むCisco TMS管理対象デバイスとの間で、暗号スイートのネゴシエーションと使用状況に問題があることを示しています。

解決方法

TMSをホストするWindowsサーバからのTransport Layer Security(TLS)接続に使用される暗号の一部が無効にされた場合、管理対象デバイスで「https応答なし」エラーを報告するCisco TMSの問題が解決されました。これにより、会議が正常に起動および監視される可能性があります。
https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-

remote-code-execution-november-11,-2014に記載されている詳細を利用する場合、Microsoftの推奨に従ってこれらの暗号を無効にすると、問題が軽減されます。

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256
```

また、TLS接続がWindowsクライアントからネゴシエートするときに問題を引き起こす可能性がある他の暗号が存在することが判明しています。詳細については、このサイトのKB3172605の問題とそのソリューションを参照してください。https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurityこれらの暗号が無効になっていると、TMSをホストするWindows ServerからのTLS接続に使用されていると、TMS管理対象デバイスでの「https応答なし」エラーの問題を解決できます。

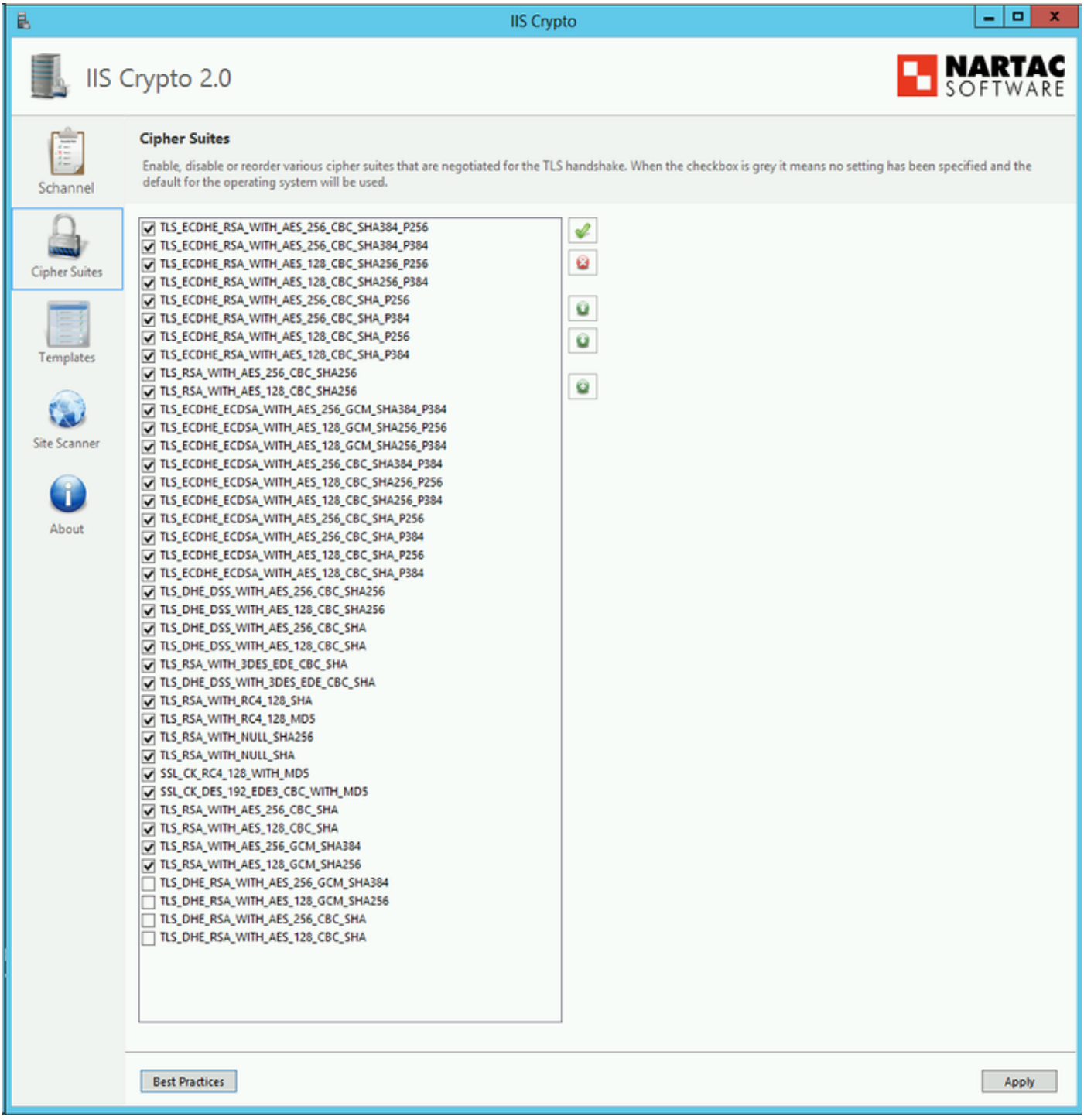
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

暗号を削除する方法は？

TMSサーバから暗号を削除する最も簡単な方法は、Internet Information Services(IIS) Cryptoというサードパーティのツールを使用することです。リストからこれらの暗号を削除してから、変更を有効にするためにTMSサーバをリブートする必要があります。ユーザがこの変更の影響を受けないように、メンテナンス時間帯のオフピーク時に行うことをお勧めします。

https://www.nartac.com/Products/IISCrypto


IIS Crypto
IIS Crypto 2.0
NARTAC SOFTWARE
Schannel
Cipher Suites
Templates
Site Scanner
About
Cipher Suites
Enable, disable or reorder various cipher suites that are negotiated for the TLS handshake. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used.
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
SSL_CK_RC4_128_WITH_MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Best Practices
Apply