TMS と OpenSSL 間の Windows 暗号原因 TLS 問題はデバイスを基づかせていました

目次

概要

この資料は Cisco TelePresence Management Suite（TMS）が管理対象装置に接続することができない、Cisco TMS で報告される「https 応答」エラーがないとき引き起こされている問題を記述したものです。 Cisco TMS は/管理するために開始するために/モニタ会議失敗します。

背景説明

TMS 解決して下さいとこのソリューションを試みる前に管理対象装置自体間の接続をされるべきです。

これらのステップは下記のものを含む必要があります:

1. TMS サーバのキャプチャ ソフトウェアを使用して下さい（前。 TMS と管理対象装置間のネットワーク接続を確認する Wireshark）。

2. これらのテクニカルノートに続いて下さい:

- 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ホスト TMS および会議ブリッジおよびエンドポイントを含む Cisco TMS 管理対象装置 Windows サーバ間の暗号スイート ネゴシエーションおよび使用状況においての問題があることを示します。

解決策

いくつかのホスト TMS が無効だった Windows サーバからの Transport Layer Security（TLS）接続に使用した暗号が、それその Cisco TMS のいくつかの問題をレポート管理対象装置のための「https 応答」エラー解決しなかった時。 これは正しく起動し、監視された会議を有効に す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 で注意される詳細を利用するとき、Microsoft の推奨事項によってディセーブルにする場合、これらの暗号を問題を軽減する可能性があります:

```
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
```

TLS 接続が Windows クライアントからネゴシエートするとき問題を引き起こす可能性がある他の暗号があるかもしれませんことがまた分られました。 詳細については、このサイトからの KB3172605 問題およびソリューションを参照して下さい: 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のとき、それはホスト TMS が、それ TMS 管理対象装置との「https 応答」エラーのいくつかの問題を解決できない Windows サーバからの TLS 接続のために使用されました:

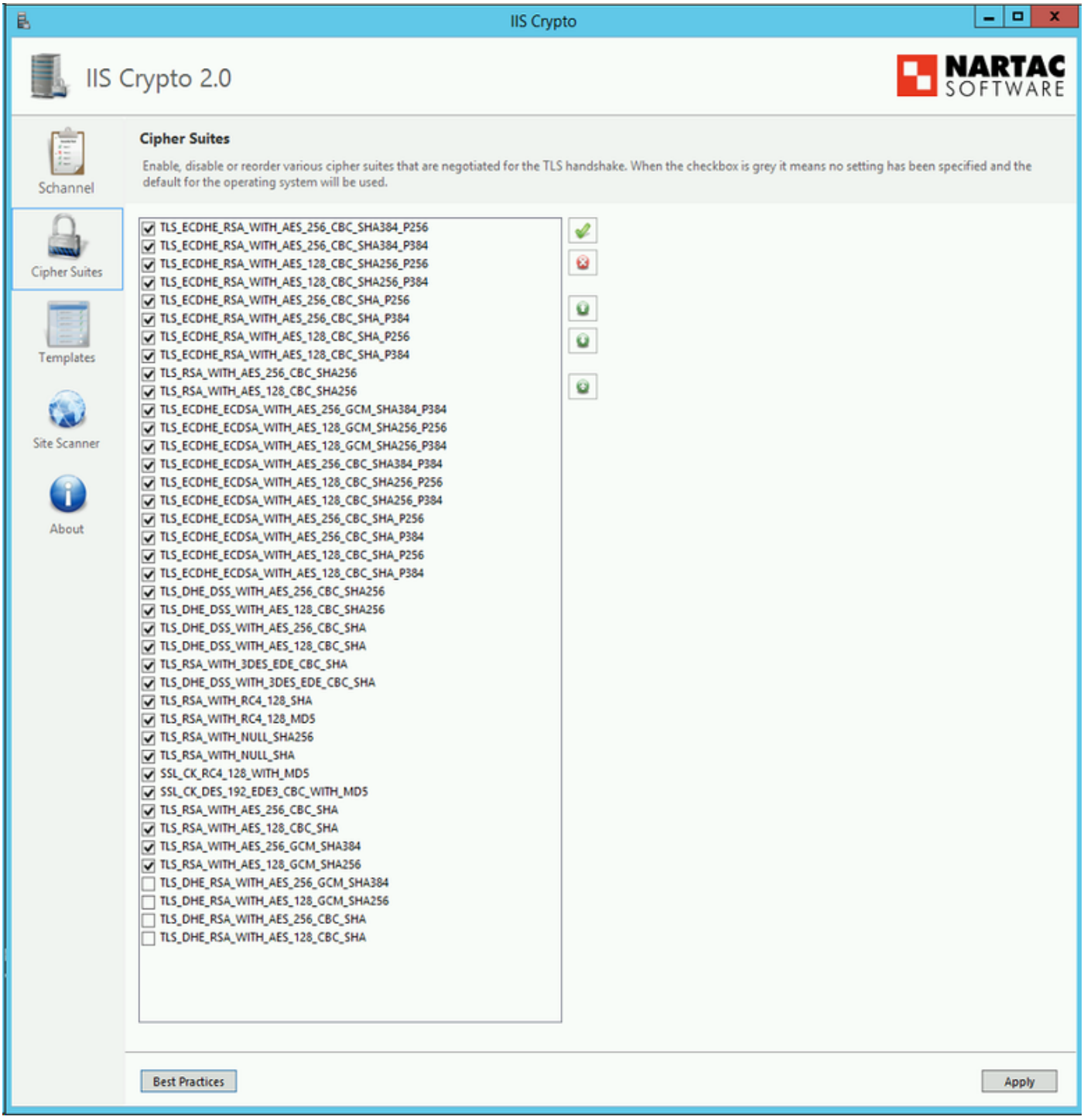
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

暗号の削除方法か。

TMS サーバから暗号を取除く最も簡単な方法は暗号 Internet Information Services （IIS）と呼ばれるサード パーティ ツールを使用することです。 リストからこれらの暗号を取除けばそれから影響を奪取 するために変更のための TMS サーバをリブートしなければなりません。 ユーザを確認するためにこれがこの変更から Maintenance ウィンドウの時にピークを過ぎた時間に影響を受けないされることを推奨します。

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