Les filtres Windows provoquent un problème de TLS entre TMS et les périphériques basés sur OpenSSL

Contenu

Introduction

Ce document décrit le problème qui se produit lorsque Cisco Telepresence Management Suite (TMS) ne peut pas se connecter à ses périphériques gérés et qu'une erreur « no https response » est signalée dans Cisco TMS. Cisco TMS ne parvient pas à démarrer/gérer/surveiller les réunions.

Informations générales

Dépannez la connectivité entre TMS et le périphérique géré lui-même avant de tenter cette solution.

Ces étapes devraient inclure :

1. Utiliser le logiciel de capture sur le serveur TMS (ex. Wireshark) pour garantir la connectivité réseau entre TMS et le périphérique géré.

2. Suivez ces notes techniques :

- 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

Problème

L'analyse d'une capture de paquets indique qu'il y a un problème avec les négociations et les utilisations de la suite Cipher entre le serveur Windows qui héberge les périphériques gérés TMS et Cisco TMS qui incluent les ponts et les terminaux de conférence.

Solution

Lorsque certains des chiffonniers utilisés pour une connexion TLS (Transport Layer Security) à partir de serveurs Windows qui hébergent TMS ont été désactivés, il a résolu certains problèmes

de Cisco TMS qui signalent une erreur « no https response » pour les périphériques gérés. Cela pourrait permettre le lancement et le suivi corrects des réunions. Lorsque vous utilisez les détails indiqués dans https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014, si vous désactivez ces Chiffres, conformément à la recommandation de Microsoft, cela pourrait atténuer le problème :

```
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
```

Il a également été découvert qu'il peut y avoir d'autres chiffrement qui pourraient causer des problèmes lorsqu'une connexion TLS négocie à partir d'un client Windows. Pour plus d'informations, référez-vous aux problèmes KB3172605 et à sa solution à partir de ce site : https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Lorsque ces chiffrement sont désactivés, qui ont été utilisés pour une connexion TLS à partir de Windows Server qui héberge TMS, il peut résoudre certains problèmes d'erreurs « no https response » avec les périphériques gérés TMS :

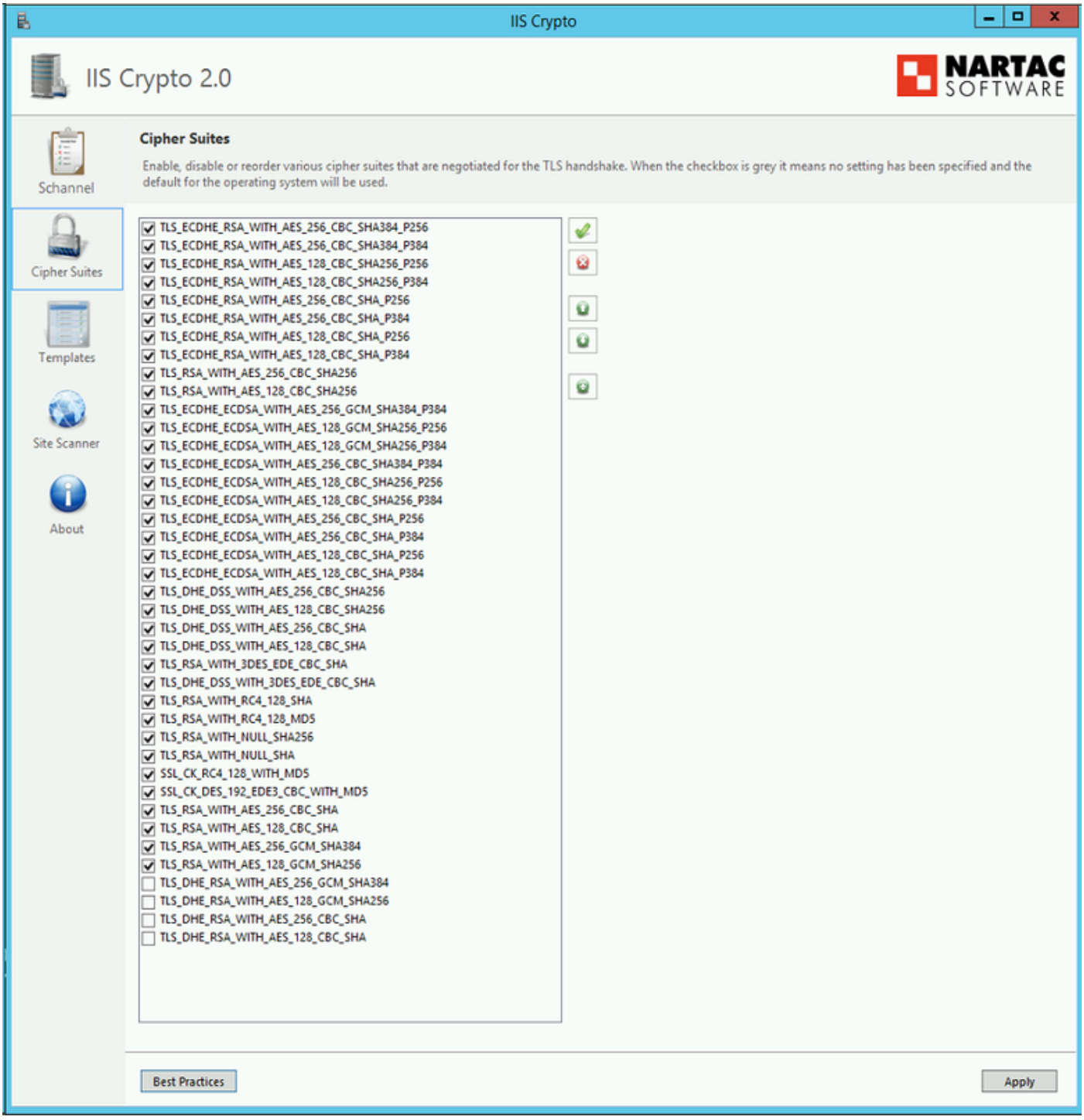
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Comment supprimer les chiffons ?

La façon la plus simple de supprimer les chiffrement du serveur TMS est d'utiliser un outil tiers appelé Crypto Internet Information Services (IIS). Supprimez ces Chiffres de la liste, puis vous devrez redémarrer le serveur TMS pour que les modifications prennent effet. Il est recommandé d'effectuer cette opération en dehors des heures de pointe au moment d'une fenêtre de maintenance afin de s'assurer que les utilisateurs ne sont pas affectés par cette modification.

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