La question de TLS de cause de chiffrements de Windows entre TMS et OpenSSL a basé des périphériques

Contenu

Introduction

Ce document décrit la question qui est provoqué par quand la suite logicielle de gestion Cisco TelePresence (TMS) ne peut pas se connecter à ses périphériques gérés et il y a une erreur de « aucune réponse de https » signalée à Cisco TMS. Cisco TMS échoue pour commencer/gérer/téléconférences de moniteur.

Informations générales

Dépannez la Connectivité entre TMS et le périphérique géré lui-même devrait être fait avant que vous tentiez cette solution.

Ces étapes devraient inclure :

1. Utilisez le logiciel de capture sur le serveur TMS (ex. Wireshark) pour assurer la connexion réseau entre TMS et le périphérique géré.

2. Suivez ces notes en tech :

- 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 paquet indique qu'il y a une question avec des négociations et des utilisations de suite de chiffrement entre les Windows Server qui hébergent TMS et périphériques gérés de Cisco TMS qui incluent des passerelles et des points finaux de Conférences.

Solution

Quand certains des chiffrements utilisés pour une connexion de Transport Layer Security (TLS)

des Windows Server qui héberge TMS ont été désactivés, ils ont résolu quelques questions de Cisco TMS qui des états erreur de « aucune réponse de https » pour les périphériques gérés. Ceci a pu permettre aux téléconférences d'être lancé et surveillé correctement. Quand vous utilisez les détails remarquables dans le 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 chiffrements, selon la recommandation de Microsoft, elle pourrait alléger la question :

```
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
```

On l'a également constaté qu'il pourrait y avoir d'autres chiffrements qui pourraient entraîner des questions quand une connexion de TLS négocie d'un client Windows. Le pour en savoir plus, se rapportent aux questions KB3172605 et à sa solution de ce site : https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Quand ces chiffrements sont désactivés, cela ont été utilisés pour une connexion de TLS des Windows Server qui hébergent TMS, il peut résoudre quelques problèmes des erreurs de « aucune réponse de https » avec des périphériques gérés TMS :

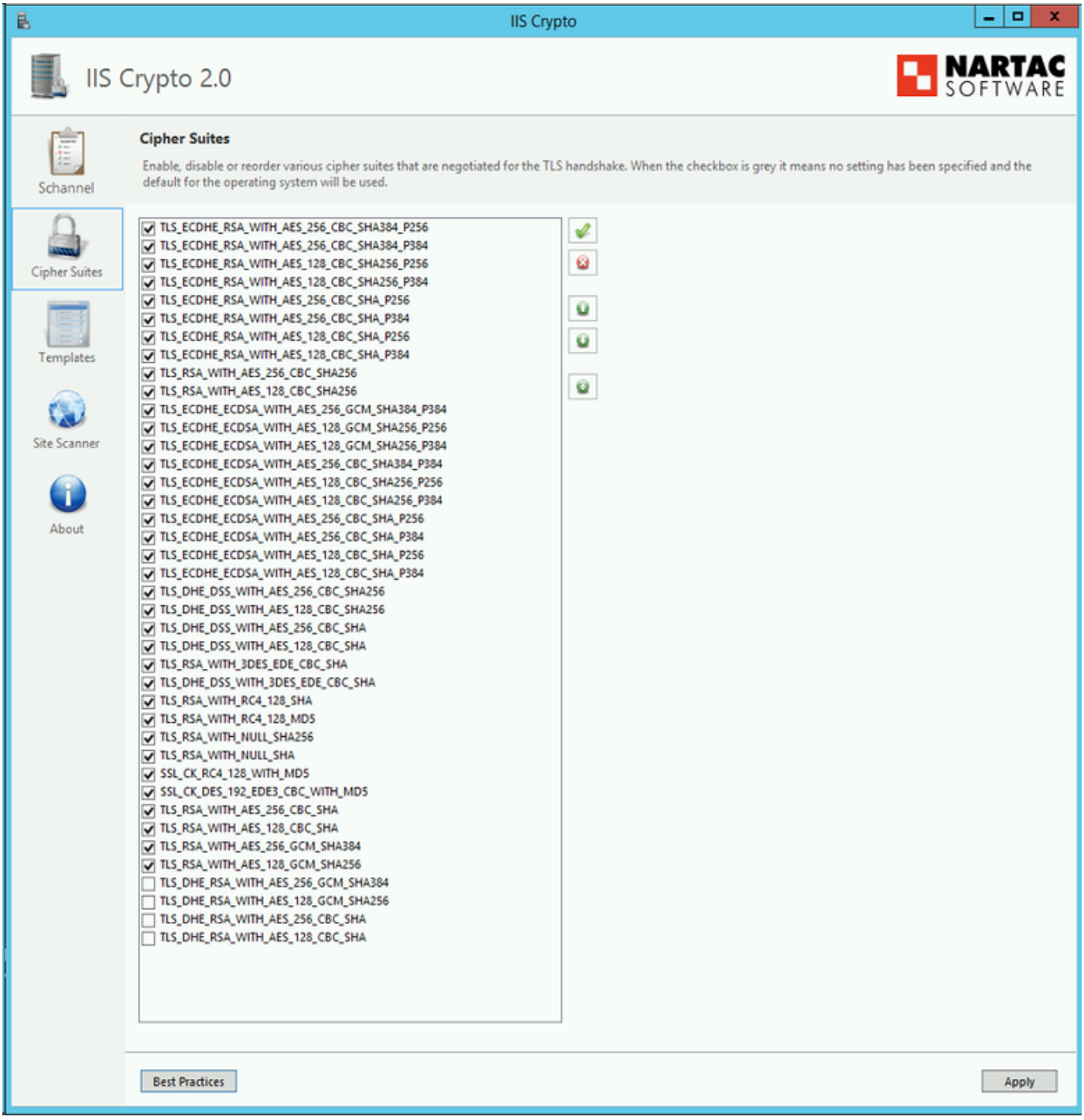
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Comment retirer les chiffrements ?

La manière la plus simple de retirer les chiffrements du serveur TMS est d'utiliser un outil de tiers appelé l'Internet Information Services (IIS) crypto. Retirez ces chiffrements de la liste et alors vous devrez redémarrer le serveur TMS pour que les modifications prennent l'affect. L'il est recommandé que ceci soit fait aux heures creuses au moment d'une fenêtre de maintenance pour s'assurer que des 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