Os clientes do Windows causam problemas de TLS entre TMS e dispositivos baseados em OpenSSL

Contents

Introduction

Este documento descreve o problema que é causado quando o Cisco Telepresence Management Suite (TMS) não consegue se conectar a seus dispositivos gerenciados e há um erro "sem resposta https" relatado no Cisco TMS. O Cisco TMS não consegue iniciar/gerenciar/monitorar reuniões.

Informações de Apoio

A solução de problemas de conectividade entre o TMS e o próprio dispositivo gerenciado deve ser feita antes que você tente esta solução.

Essas etapas devem incluir:

1. Use o software de captura no servidor TMS (ex. Wireshark) para garantir a conectividade de rede entre o TMS e o dispositivo gerenciado.

2. Siga estas notas técnicas:

- 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

Problema

A análise de uma captura de pacote indica que há um problema com as negociações e usos do pacote de Cipher entre o servidor Windows que hospeda dispositivos gerenciados TMS e Cisco TMS que incluem pontes de conferência e endpoints.

Solução

Quando alguns dos Ciphers usados para uma conexão TLS (Transport Layer Security) de

servidores Windows que hospedam o TMS foram desabilitados, resolveu alguns problemas do Cisco TMS que relatam o erro "no https response" (não há resposta https) para os dispositivos gerenciados. Isso pode permitir que as reuniões sejam iniciadas e monitoradas corretamente. Ao utilizar os detalhes anotados em https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014, se você desativar esses Ciphers, de acordo com a recomendação da Microsoft, isso poderá aliviar o problema:

```
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
```

Também foi descoberto que pode haver outros Cifras que podem causar problemas quando uma conexão TLS negocia de um cliente Windows. Para obter mais informações, consulte os problemas do KB3172605 e sua solução neste site: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Quando esses Ciphers são desabilitados, que foram usados para uma conexão TLS do Windows Server que hospeda o TMS, ele pode resolver alguns problemas dos erros "sem resposta https" com dispositivos gerenciados do TMS:

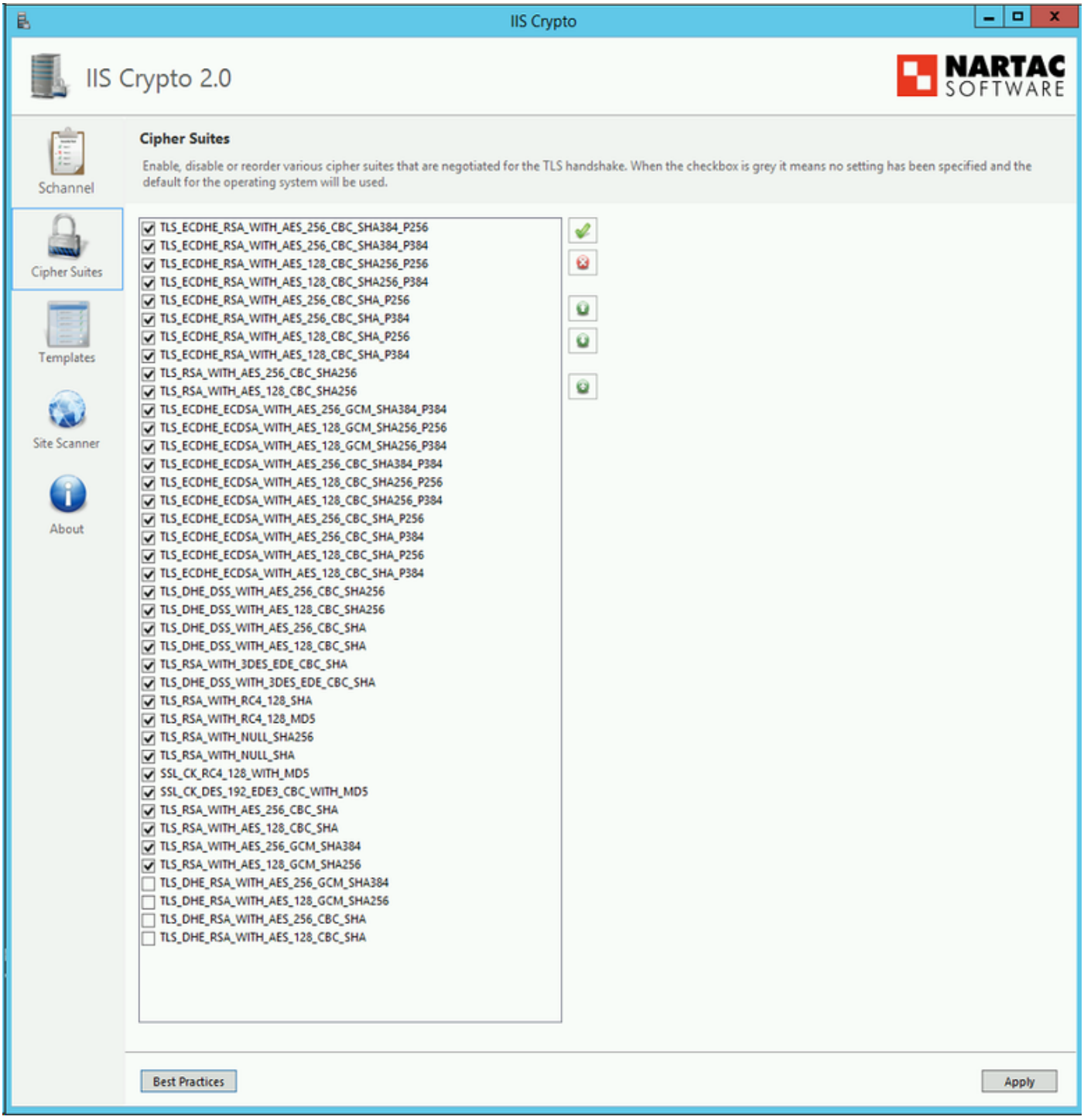
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Como remover os Ciphers?

A maneira mais simples de remover os Ciphers do Servidor TMS é usar uma ferramenta de terceiros chamada Internet Information Services (IIS) Crypto. Remova esses Cifras da lista e você terá que reinicializar o Servidor TMS para que as alterações entrem em vigor. Recomenda-se que isso seja feito fora das horas de pico no momento de uma janela de manutenção para garantir que os usuários não sejam afetados por essa alteração.

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