A edição da causa TLS das cifras de Windows entre TMS e OpenSSL baseou dispositivos

Índice

Introdução

Este documento descreve a edição que está causada quando a suite de gerenciamento do Cisco TelePresence (TMS) é incapaz de conectar a seus dispositivos gerenciado e lá é de “um erro nenhuma resposta dos https” relatado em Cisco TMS. Cisco TMS começar/não controla/reuniões do monitor.

Informações de Apoio

Pesquise defeitos a Conectividade entre TMS e o dispositivo gerenciado próprio deve ser feito antes que você tente esta solução.

Estas etapas devem incluir:

1. Use o software da captação no server TMS (ex. Wireshark) para assegurar a conectividade de rede entre TMS e o dispositivo gerenciado.

2. Siga estas Notas Técnica:

- 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 de informação indica que há uma edição com negociações e usos da série da cifra entre o Windows Server que hospedam TMS e dispositivos gerenciado de Cisco TMS que incluem pontes e valores-limite das Conferências.

Solução

Quando algumas das cifras usadas para uma conexão do Transport Layer Security (TLS) dos Windows Server que hospedasse TMS foram desabilitadas, resolveram algumas introduções de Cisco TMS esse relatórios de “erro nenhuma resposta dos https” para os dispositivos gerenciado.

Isto podia permitir as reuniões de ser lançado corretamente e monitorado. Quando você utiliza os detalhes notáveis no https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014, se você desabilita estas cifras, conforme a recomendação de Microsoft, poderia aliviar a edição:

```
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
```

Igualmente encontrou-se que pôde haver outras cifras que poderiam causar edições quando uma conexão TLS negocia de um cliente do Windows. Para mais informação, refira as edições KB3172605 e a sua solução deste local: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Quando estas cifras são desabilitadas, aquela esteve usada para uma conexão TLS de Windows Server que hospedasse TMS, ele pode resolver algumas introduções de “dos erros nenhuma resposta dos https” com dispositivos gerenciado TMS:

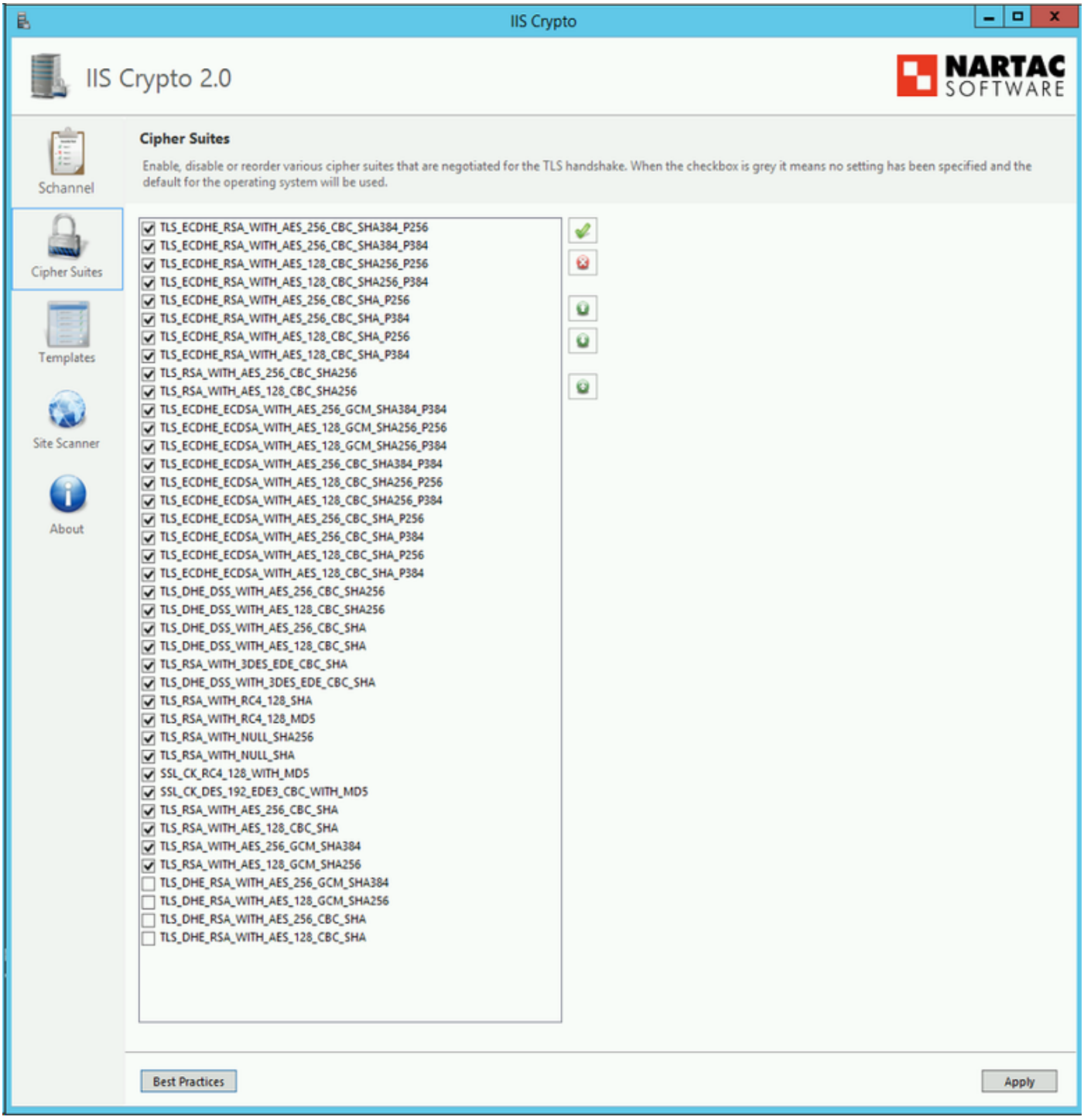
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Como remover as cifras?

A maneira a mais simples de remover as cifras do server TMS é usar uma ferramenta da terceira parte chamada o Internet Information Services (IIS) cripto. Remova estas cifras da lista e então você terá que recarregar o server TMS para que as mudanças tomem a influência. Recomenda-se que este esteja feito em horas fora de pico na altura de uma janela de manutenção para se assegurar de que os usuários não estejam afetados por esta mudança.

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