El problema de TLS de la causa de las cifras de Windows entre TMS y el OpenSSL basó los dispositivos

Contenido

Introducción

Este documento describe el problema se causa que cuando el conjunto de administración del Cisco TelePresence (TMS) no puede conectar con sus dispositivos administrados y allí es un error de “ninguna respuesta del https” señalado en Cisco TMS. Cisco TMS no puede comenzar/para manejar/las reuniones del monitor.

Antecedentes

La Conectividad del Troubleshooting entre TMS y el dispositivo administrado sí mismo debe ser hecha antes de que usted intente esta solución.

Estos pasos deben incluir:

1. Utilice el software de la captura en el servidor TMS (ex. Wireshark) para asegurar la conectividad de red entre TMS y el dispositivo administrado.

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

El análisis de una captura de paquetes indica que hay un problema con las negociaciones y los usos de la habitación de la cifra entre el Servidor Windows que reciben TMS y los dispositivos administrados de Cisco TMS que incluyan los Bridges y los puntos finales de la Conferencia.

Solución

Cuando algunas de las cifras usadas para una conexión de Transport Layer Security (TLS) de los

Servidores Windows que recibe TMS fueron inhabilitadas, resolvieron algunas aplicaciones Cisco TMS ese los informes error de “ninguna respuesta del https” para los dispositivos administrados. Esto podía habilitar las reuniones que se iniciarán y monitoreadas correctamente. Cuando usted utiliza los detalles conocidos en el https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014, si usted inhabilita estas cifras, según la recomendación de Microsoft, podría paliar el 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
```

También se ha encontrado que pudo haber otras cifras que podrían causar los problemas cuando una conexión TLS negocia de un cliente de Windows. Para más información, refiera a los problemas KB3172605 y a su solución de este sitio: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Cuando se inhabilitan estas cifras, eso se ha utilizado para una conexión TLS del Servidor Windows que recibe TMS, él puede resolver algunas aplicaciones los errores de “ninguna respuesta del https” con los dispositivos administrados TMS:

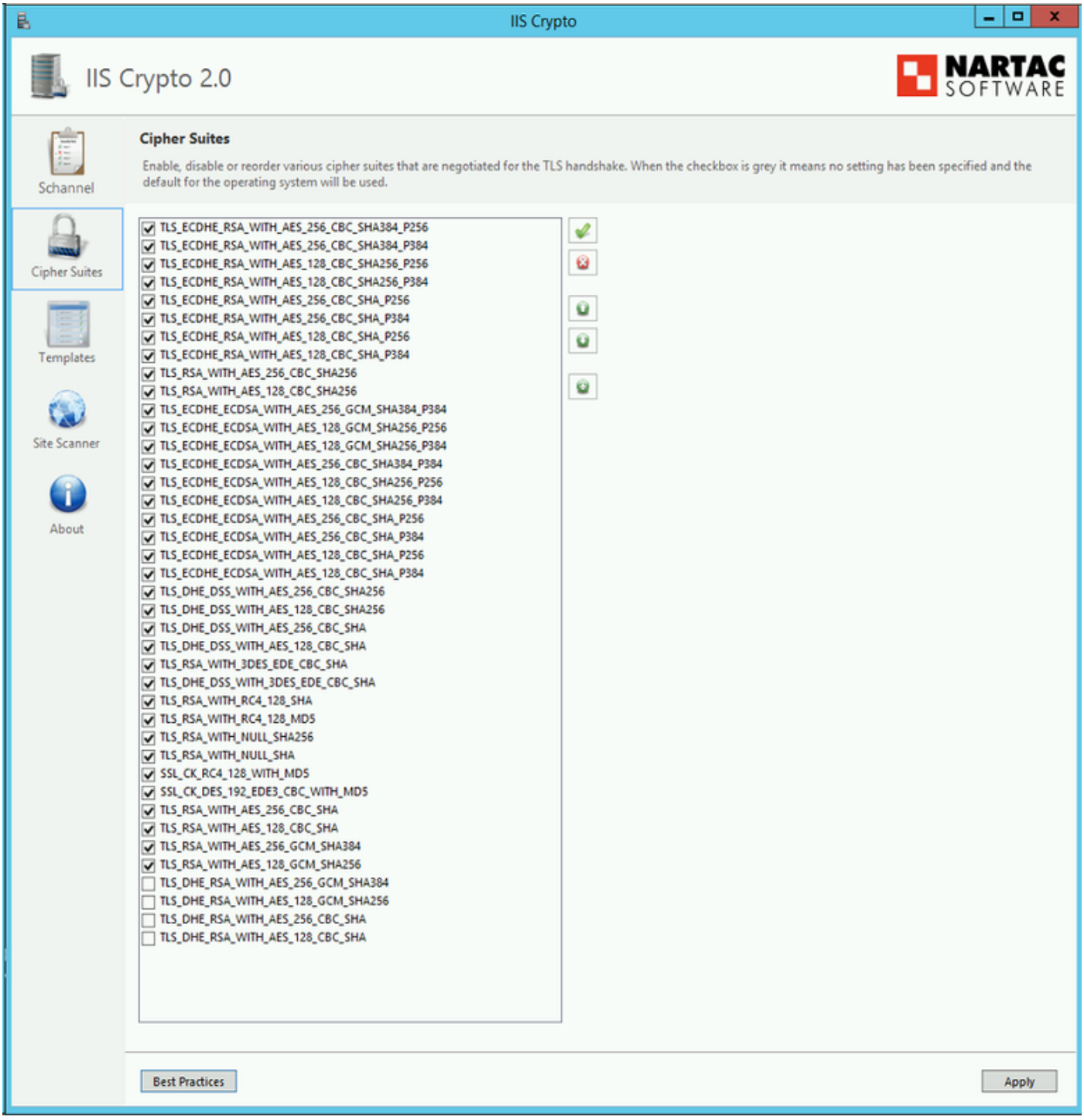
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

¿Cómo quitar las cifras?

La manera más simple de quitar las cifras del servidor TMS es utilizar una herramienta del otro vendedor llamada los Servicios de Internet Information Server (IIS) Crypto. Quite estas cifras de la lista y entonces usted tendrá que reiniciar el servidor TMS para que los cambios tomen la influencia. Se recomienda que éste esté hecho en las horas huecas a la hora de una ventana de mantenimiento para asegurarse que este cambio no afectan a los usuarios.

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