Los cifradores de Windows provocan un problema de TLS entre los dispositivos basados en TMS y OpenSSL

Contenido

[Introducción](#)
[Antecedentes](#)
[Problema](#)
[Solución](#)

Introducción

Este documento describe el problema que se produce cuando Cisco Telepresence Management Suite (TMS) no puede conectarse a sus dispositivos administrados y se informa de un error de "no https response" en Cisco TMS. Cisco TMS no puede iniciar/administrar/supervisar reuniones.

Antecedentes

Debe resolver problemas de conectividad entre TMS y el propio dispositivo administrado antes de intentar esta solución.

Estas medidas deberían incluir:

1. Utilice el software de captura en el servidor TMS (p. ej. Wireshark) para garantizar 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 del conjunto de aplicaciones Cipher y los usos entre el servidor Windows que alojan TMS y los dispositivos gestionados por Cisco TMS que incluyen puentes de conferencia y terminales.

Solución

Cuando se desactivaron algunos de los Ciphers utilizados para una conexión de seguridad de la capa de transporte (TLS) de los servidores de Windows que alojan TMS, se resolvieron algunos

problemas de Cisco TMS que informan del error "no https response" para los dispositivos administrados. Esto podría permitir que las reuniones se iniciaran y supervisaran correctamente. Cuando utiliza los detalles indicados en https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014, si inhabilita estos Cifers, según la recomendación de Microsoft, podría aliviar 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 podría haber otros Ciphers que podrían causar problemas cuando una conexión TLS negocia desde un cliente de Windows. Para obtener más información, consulte los problemas de KB3172605 y su solución desde este sitio: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Cuando estos Ciphers están inhabilitados, que se han utilizado para una conexión TLS desde Windows Server que aloja TMS, puede resolver algunos problemas de los errores "sin respuesta https" con los dispositivos administrados TMS:

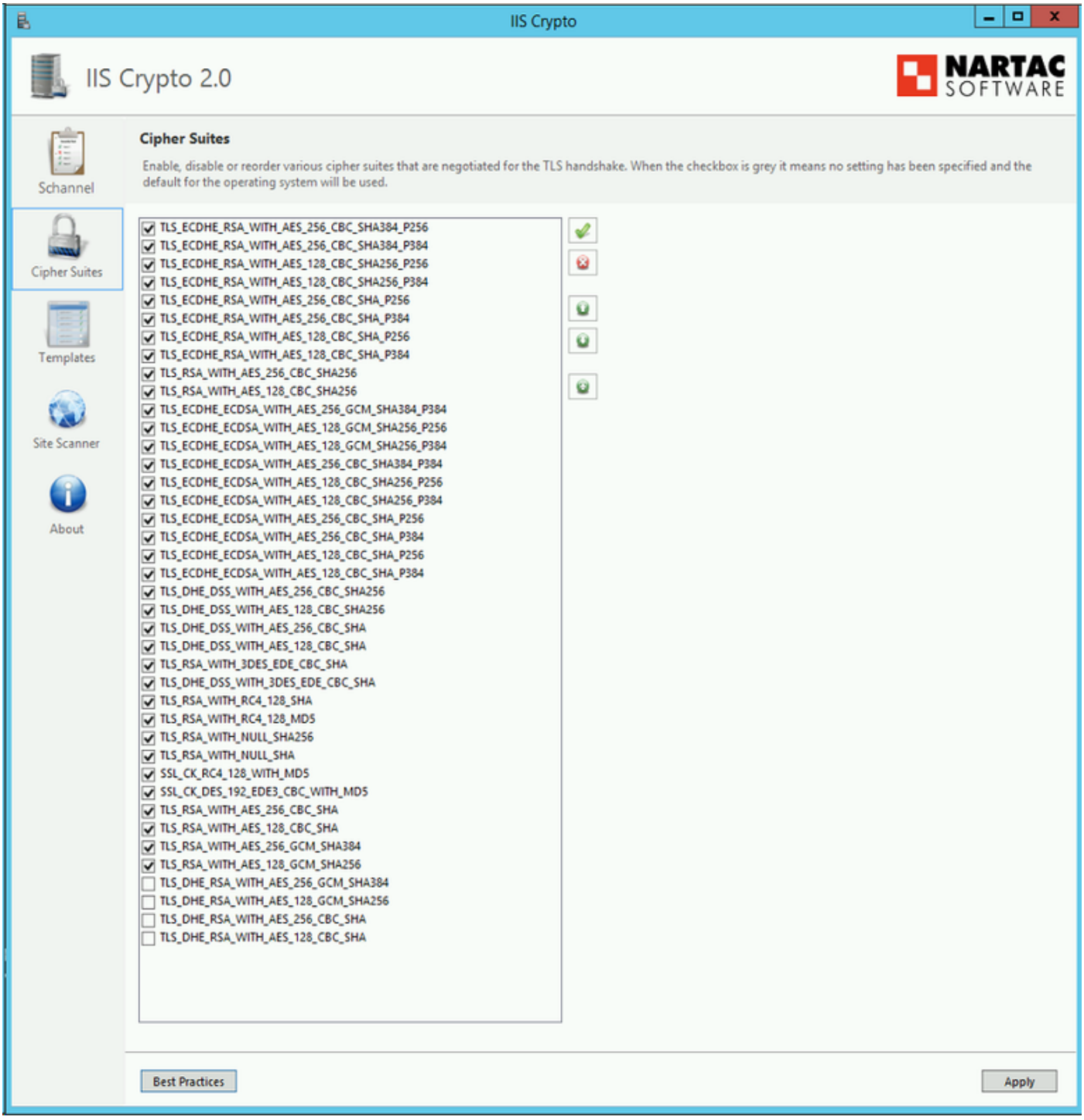
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

¿Cómo eliminar los Cifradores?

La forma más sencilla de quitar los cifradores del servidor TMS es utilizar una herramienta de terceros llamada Internet Information Services (IIS) Crypto. Quite estos Cifradores de la lista y después tendrá que reiniciar el servidor TMS para que los cambios surtan efecto. Se recomienda que esto se haga fuera de las horas punta en el momento de una ventana de mantenimiento para asegurarse de que los usuarios no se vean afectados por este cambio.

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