Problemi di crittografia Windows tra dispositivi basati su TMS e OpenSSL

Sommario

Introduzione

Questo documento descrive il problema causato da Cisco Telepresence Management Suite (TMS) nell'impossibilità di connettersi ai suoi dispositivi gestiti e un errore "no https response" segnalato in Cisco TMS. Cisco TMS non riesce ad avviare/gestire/monitorare le riunioni.

Premesse

Prima di provare questa soluzione, è necessario risolvere i problemi di connettività tra TMS e il dispositivo gestito stesso.

Tali misure dovrebbero comprendere:

1. Utilizzare il software di acquisizione sul server TMS (es. Wireshark) per garantire la connettività di rete tra TMS e il dispositivo gestito.

2. Attenersi alle seguenti note tecniche:

- 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

L'analisi di un'acquisizione di pacchetti indica che esiste un problema con le negoziazioni e gli utilizzi della suite di cifratura tra il server Windows che ospita dispositivi gestiti TMS e Cisco TMS che includono bridge per conferenze ed endpoint.

Soluzione

Quando alcune delle cifrature utilizzate per una connessione Transport Layer Security (TLS) dai server Windows che ospitano TMS sono state disabilitate, sono stati risolti alcuni problemi di Cisco TMS che segnalano l'errore "nessuna risposta https" per i dispositivi gestiti. In questo modo le riunioni potrebbero essere avviate e monitorate correttamente. Se si utilizzano i dettagli indicati

in https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014, la disattivazione di questi filtri, in base ai suggerimenti di Microsoft, potrebbe ridurre il 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
```

Èstato inoltre rilevato che potrebbero esistere altri tipi di crittografia che causano problemi quando una connessione TLS esegue la negoziazione da un client Windows. Per ulteriori informazioni, fare riferimento ai problemi di KB3172605 e alla relativa soluzione da questo sito: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Quando queste cifrature sono disattivate, che sono state utilizzate per una connessione TLS da Windows Server che ospita TMS, può risolvere alcuni problemi di "no https response" error con i dispositivi gestiti TMS:

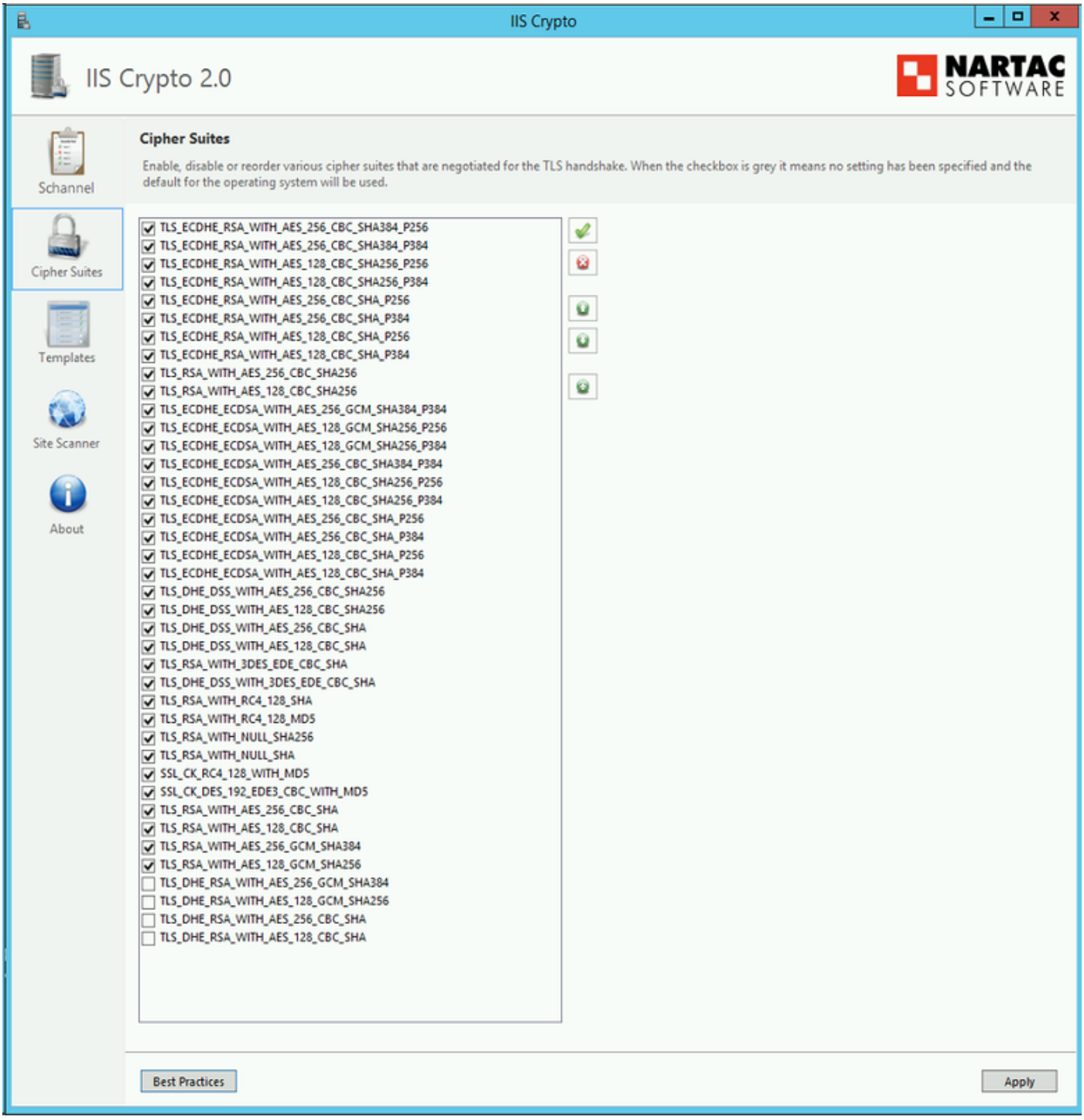
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Come rimuovere i cifrari?

Il modo più semplice per rimuovere le cifrature dal server TMS consiste nell'utilizzare uno strumento di terze parti denominato Crittografia di Internet Information Services (IIS). Rimuovere queste cifrature dall'elenco, quindi riavviare il server TMS per rendere effettive le modifiche. Si consiglia di eseguire questa operazione nelle ore non di punta durante un intervento di manutenzione per garantire che gli utenti non siano interessati da questa modifica.

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