Windows CIPS-problemen veroorzaken tussen TMS- en OpenSSL-apparaten

Inhoud

Inleiding

Dit document beschrijft de kwestie die wordt veroorzaakt wanneer Cisco TelePresence Management Suite (TMS) niet kan worden aangesloten op zijn beheerde apparaten en er is een fout "no https Response" gemeld in Cisco TMS. Cisco TMS kan geen vergaderingen starten/beheren/bewaken.

Achtergrondinformatie

De verbinding van de probleemoplossing tussen TMS en het beheerde apparaat zelf zou moeten worden gedaan alvorens u deze oplossing probeert.

Deze maatregelen moeten het volgende omvatten:

1. Gebruik opnamesoftware op de TMS Server (bijvoorbeeld). Wireshark) om netwerkconnectiviteit tussen TMS en het beheerde apparaat te verzekeren.

2. Volg deze technische opmerkingen:

- 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

Probleem

De analyse van een pakketvastlegging geeft aan dat er een probleem is met onderhandelingen in de Cisco-suite en gebruik tussen de Windows-server waarop TMS en Cisco TMS beheerde apparaten worden ontvangen, zoals conferencing-bruggen en endpoints.

Oplossing

Wanneer sommige van de Ciphers voor een verbinding van de Veiligheid van de Transport Layer (TLS) van de servers van Windows die TMS huurden werden gehandicapt, lost het sommige kwesties van Cisco TMS op die "geen "https respons" fout voor de beheerde apparaten meldt. Dit

zou het mogelijk kunnen maken de vergaderingen correct te lanceren en te controleren. Wanneer u de details in https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014 gebruikt, als u deze CIFERS uitschakelt, zoals wordt aanbevolen door Microsoft, zou dit de kwestie kunnen verlichten:

```
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
```

Er zijn ook andere ciphers gevonden die problemen kunnen veroorzaken wanneer een TLS-verbinding van een Windows client onderhandelt. Zie voor meer informatie KB3172605-kwesties en de oplossing ervan op deze site: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Wanneer deze Cifers worden uitgeschakeld, die zijn gebruikt voor een TLS-verbinding vanuit Windows Server die TMS gastheer is, kan het een aantal problemen van de "no https-respons"-fouten oplossen met TMS-beheerde apparaten:

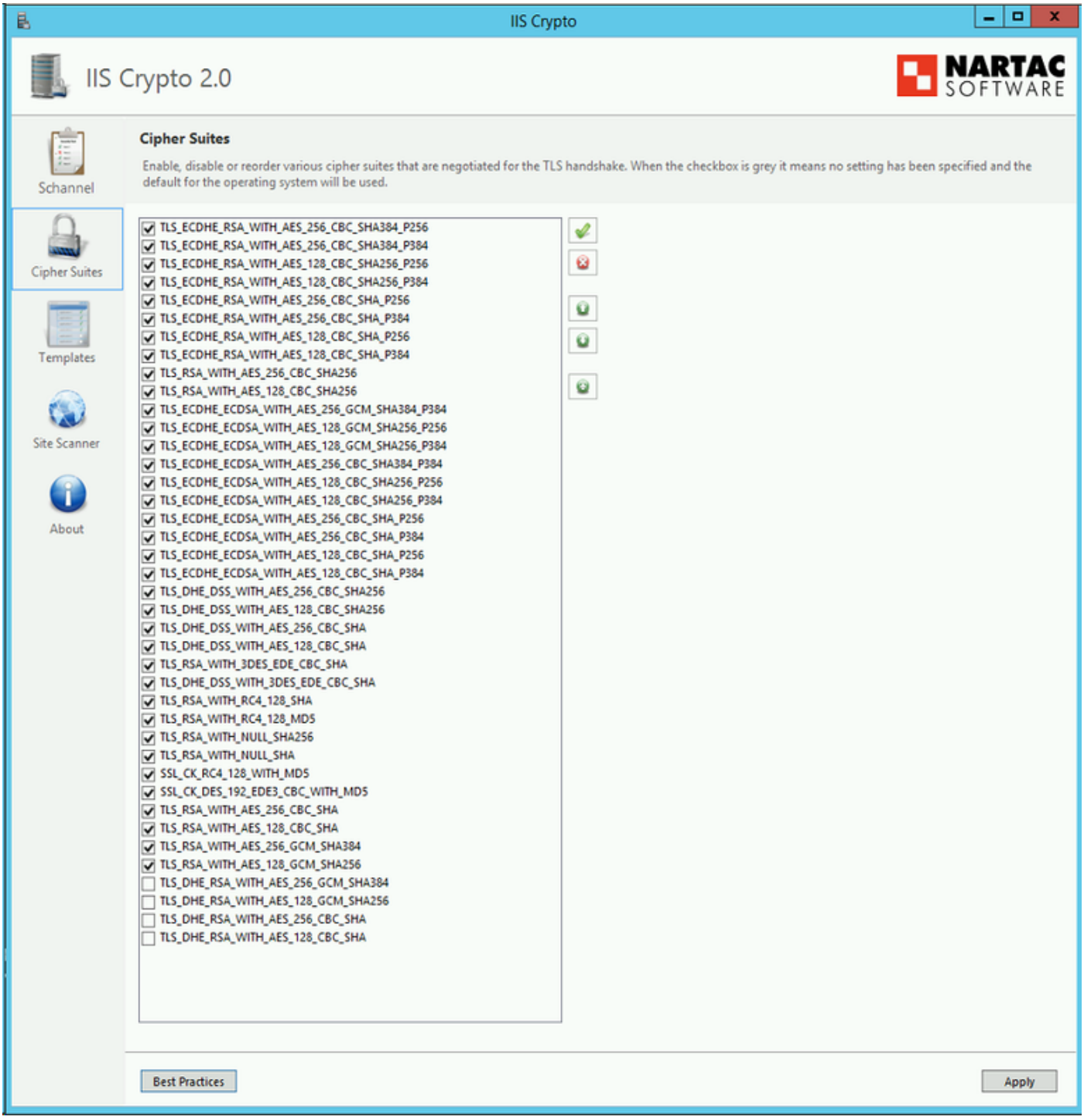
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Hoe de civilen te verwijderen?

De eenvoudigste manier om de CIFERS van de TMS Server te verwijderen is door het gebruik van een derdengereedschap genaamd Internet Information Services (IS) Crypto. Verwijder deze CIJFERS uit de lijst en start de TMS Server opnieuw om de wijzigingen door te voeren. Aanbevolen wordt dit te doen op het moment van een onderhoudsvenster tijdens de piekuren om er zeker van te zijn dat de gebruikers niet door deze verandering worden beïnvloed.

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