Windows-Chiffren verursachen TLS-Probleme zwischen TMS und OpenSSL-basierten Geräten.

Inhalt

Einführung

In diesem Dokument wird das Problem beschrieben, das verursacht wird, wenn die Cisco Telepresence Management Suite (TMS) keine Verbindung zu den verwalteten Geräten herstellen kann. In Cisco TMS wird der Fehler "no https response" (Keine HTTPS-Antwort) gemeldet. Cisco TMS kann Meetings nicht starten/verwalten/überwachen.

Hintergrundinformationen

Die Fehlerbehebung für die Verbindung zwischen dem TMS und dem verwalteten Gerät selbst sollte vor dem Versuch dieser Lösung durchgeführt werden.

Diese Schritte sollten Folgendes umfassen:

1. Verwenden Sie die Erfassungssoftware auf dem TMS-Server (z. B. Wireshark), um die Netzwerkverbindung zwischen TMS und dem verwalteten Gerät sicherzustellen.

2. Befolgen Sie diese technischen Hinweise:

- 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

Problem

Die Analyse einer Paketerfassung weist darauf hin, dass bei den Cipher Suite-Aushandlungen und -Verwendungen zwischen dem Windows-Server, der TMS hostet, und den verwalteten Cisco TMS-Geräten, zu denen auch Konferenzbrücken und Endpunkte gehören, ein Problem besteht.

Lösung

Wenn einige der Ciphers für eine TLS-Verbindung (Transport Layer Security) von Windows-Servern, die TMS hostet, deaktiviert wurden, wurden einige Probleme von Cisco TMS behoben, die für die verwalteten Geräte den Fehler "no https response" (Keine HTTPS-Antwort) melden.

Dadurch können Meetings ordnungsgemäß gestartet und überwacht werden. Wenn Sie die unter https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014 angegebenen Details verwenden, können Sie diese Chiffren gemäß der Empfehlung von Microsoft deaktivieren, um das Problem zu beheben:

```
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
```

Es wurde außerdem festgestellt, dass es möglicherweise weitere Ciphers gibt, die Probleme verursachen können, wenn eine TLS-Verbindung von einem Windows-Client aus ausgehandelt wird. Weitere Informationen finden Sie im Dokument KB3172605-Probleme und deren Lösung von dieser Seite: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. Wenn diese Ciphers deaktiviert sind, die für eine TLS-Verbindung von Windows Server verwendet wurden, der TMS hostet, können einige Probleme mit den Fehlern "keine HTTPS-Antwort" bei verwalteten TMS-Geräten behoben werden:

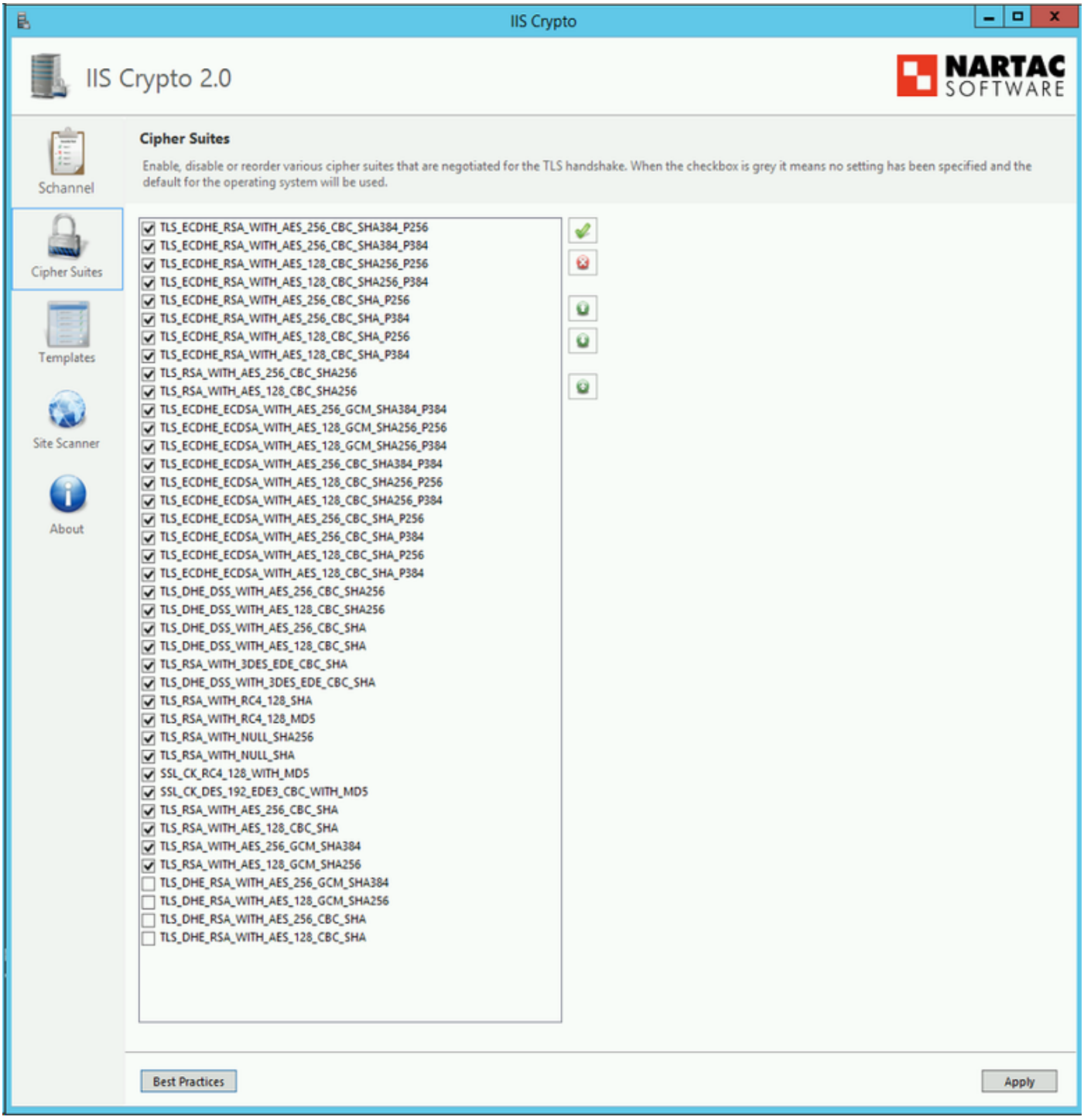
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Wie werden die Chiffren entfernt?

Die einfachste Möglichkeit, die Chiffren aus dem TMS-Server zu entfernen, ist die Verwendung eines Drittanbietertools namens Internet Information Services (IIS) Crypto. Entfernen Sie diese Ciphers aus der Liste, und dann müssen Sie den TMS-Server neu starten, damit die Änderungen wirksam werden. Es wird empfohlen, dies zu Nebenzeiten während eines Wartungsfensters zu tun, um sicherzustellen, dass die Benutzer von dieser Änderung nicht betroffen sind.

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