تتسبب تشفير Windows في حدوث مشاكل TLS بين TMS والأجهزة المستندة إلى OpenSSL

المحتويات

المقدمة

يصف هذا المستند المشكلة التي تحدث عندما يتعذر على Cisco TelePresence Management Suite (TMS) الاتصال بأجهزته المدارة وهناك خطأ "no https response" تم الإعلام عنه في Cisco TMS. فشل Cisco TMS في بدء/إدارة/مراقبة الاجتماعات.

معلومات أساسية

يجب إجراء أستكشاف أخطاء الاتصال وإصلاحها بين TMS والجهاز المدار نفسه قبل محاولة إجراء هذا الحل.

يجب أن تشمل هذه الخطوات ما يلي:

1. أستخدم برنامج الالتقاط على خادم TMS (على سبيل المثال Wireshark) لضمان اتصال الشبكة بين TMS والجهاز المدار.

2. اتبع هذه الملاحظات الفنية:

- 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

المشكلة

يشير تحليل التقاط حزمة إلى وجود مشكلة في مفاوضات مجموعة التشفير واستخدامها بين خادم Windows الذي يستضيف TMS والأجهزة المدارة من Cisco TMS التي تتضمن جسور المؤتمرات ونقاط النهاية.

الحل

عندما تم تعطيل بعض التشفير المستخدم لاتصال "أمان طبقة النقل (TLS)" من خوادم Windows التي تستضيف TMS، تم حل بعض مشاكل Cisco TMS التي تشير إلى خطأ "ال

إستجابة HTTPS" للأجهزة المدارة. قد يؤدي ذلك إلى تمكين تشغيل الاجتماعات ومراقبتها بشكل صحيح. عند إستخدام التفاصيل المشار إليها في https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014، إذا قمت بتعطيل هذه التشفير، وفقا لتوصية Microsoft، فقد يؤدي ذلك إلى تخفيف المشكلة:

```
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
```

كما تم العثور على إمكانية وجود شفرات أخرى قد تتسبب في مشاكل عند تفاوض اتصال TLS من عميل Windows. لمزيد من المعلومات، ارجع إلى مشاكل KB3172605 وحلولها من هذا الموقع: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. عندما يتم تعطيل هذه التشفير، والذي تم إستخدامه لاتصال TLS من خادم Windows الذي يستضيف TMS، يمكن حل بعض مشاكل أخطاء "عدم إستجابة https" مع الأجهزة التي تتم إدارتها بواسطة TMS:

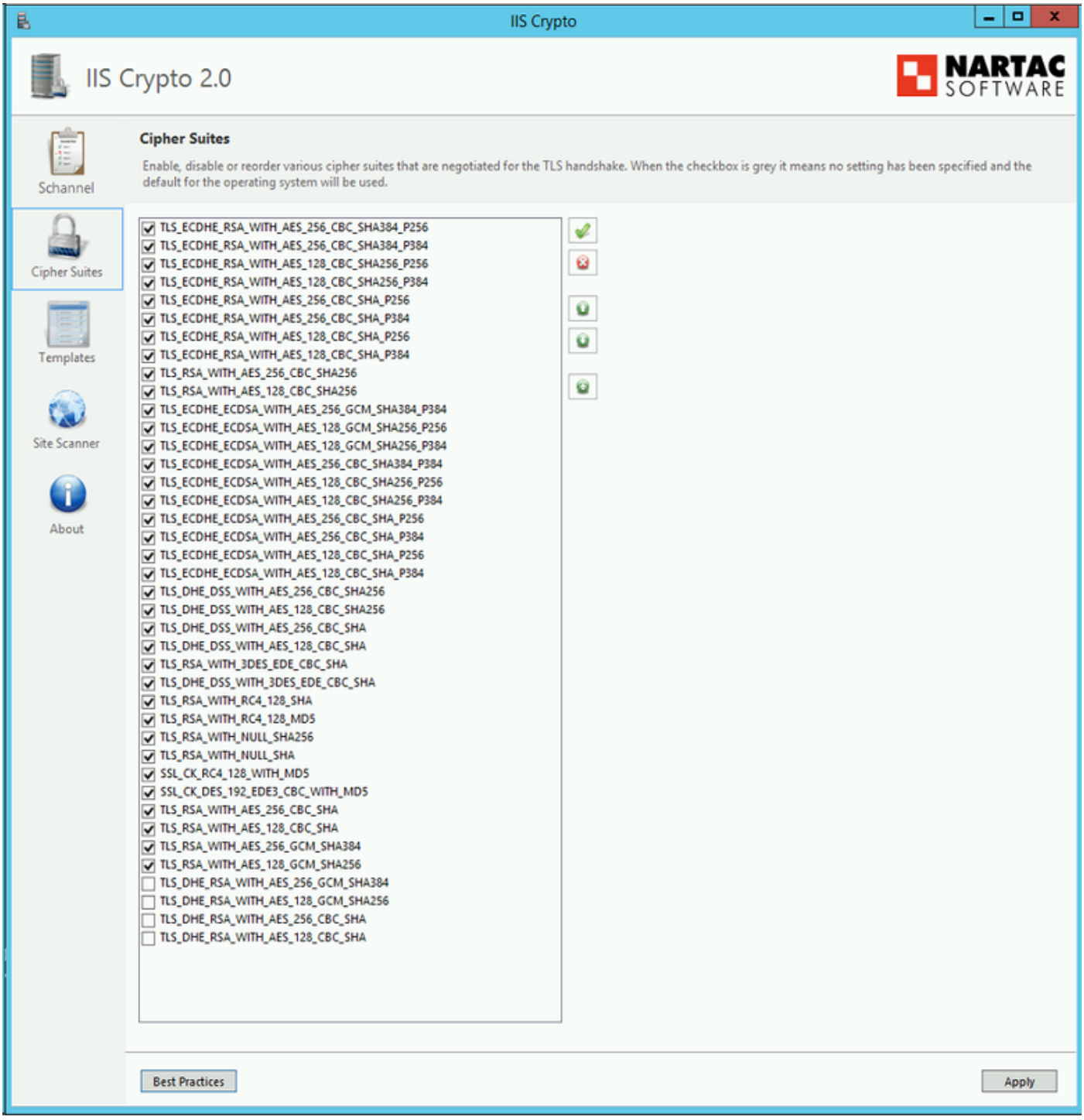
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

كيف نزيل الشفرات؟

وأبسط طريقة لإزالة المشفرة من خادم TMS هي إستخدام أداة طرف ثالث تسمى تشفير أو خدمات معلومات الإنترنت (IIS). قم بإزالة هذه الشفرات من القائمة، ثم سيتعين عليك إعادة تشغيل خادم TMS لكي تؤثر التغييرات. ويوصى بالقيام بذلك في ساعات الذروة في وقت وجود إطار الصيانة لضمان عدم تأثر المستخدمين بهذا التغيير.

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).