Windows Ciphers Cause TLS Issue between TMS and OpenSSL Based Devices

Contents

Introduction

This document describes the issue that is caused when Cisco Telepresence Management Suite (TMS) is unable to connect to its managed devices and there is a "no https response" error reported in Cisco TMS. Cisco TMS fails to start/manage/monitor meetings.

Background Information

Troubleshoot connectivity between TMS and the managed device itself should be done before you attempt this solution.

These steps should include:

1. Use capture software on the TMS Server (ex. Wireshark) to ensure network connectivity between TMS and the managed device.

2. Follow these Tech Notes:

- 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

The analysis of a packet capture indicates that there is an issue with Cipher suite negotiations and usages between the Windows server that host TMS and Cisco TMS managed devices that include conferencing bridges and endpoints.

Solution

When some of the Ciphers used for a Transport Layer Security (TLS) connection from Windows Servers that hosts TMS were disabled, it resolved some issues of Cisco TMS that reports "no https response" error for the managed devices. This could enable the meetings to be launched and monitored correctly. When you utilize the details noted in https://support.microsoft.com/en-

us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014, if you disable these Ciphers, as per Microsoft's recommendation, it could alleviate the issue:

```
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
```

It has also been found that there might be other Ciphers that could cause issues when a TLS connection negotiates from a Windows client. For more information, refer to KB3172605 issues and its solution from this site: https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity. When these Ciphers are disabled, that have been used for a TLS connection from Windows Server that hosts TMS, it can resolve some issues of the "no https response" errors with TMS managed devices:

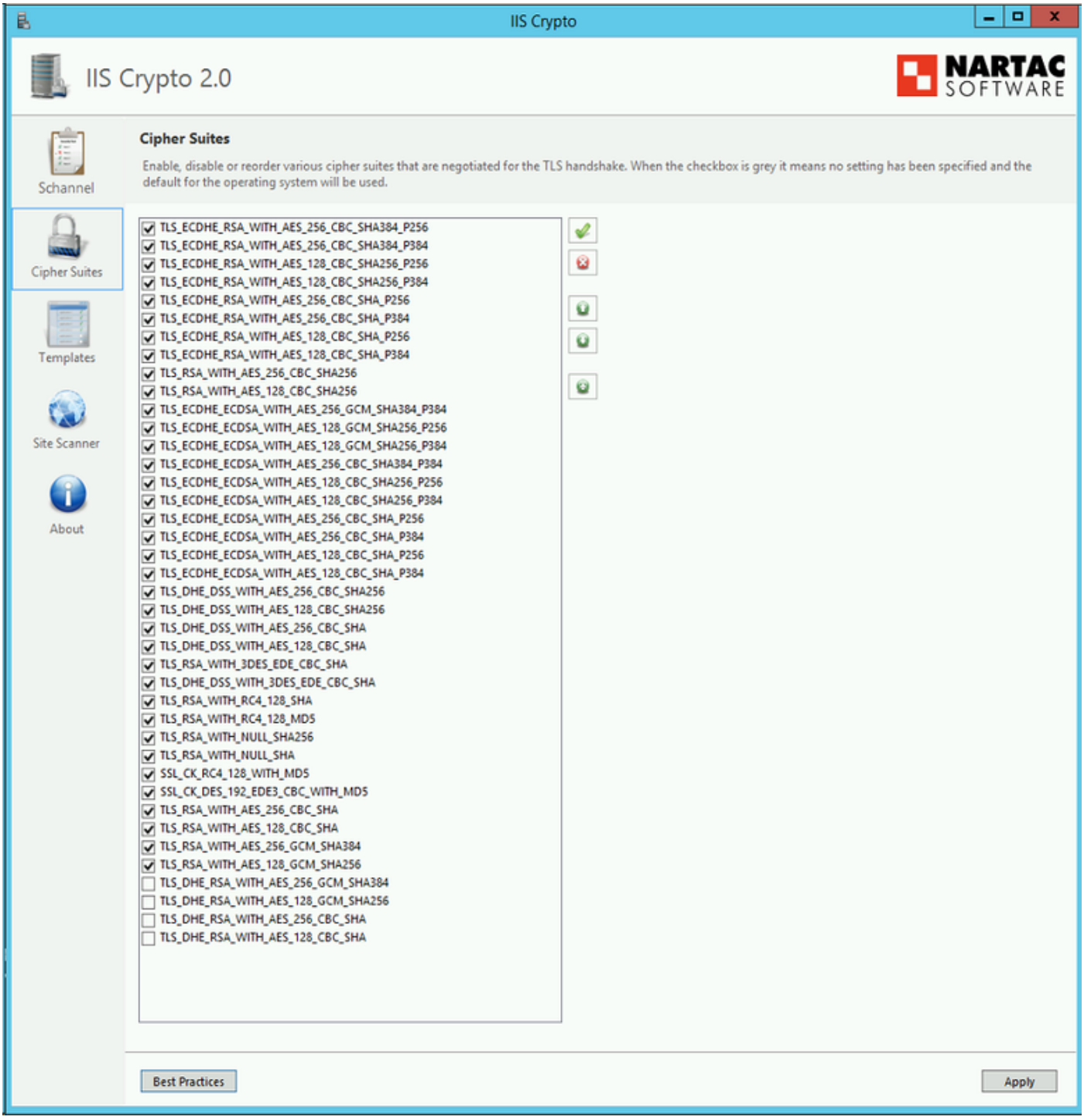
```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

How to remove the Ciphers?

The simplest way to remove the Ciphers from the TMS Server is to use a third party tool called Internet Information Services (IIS) Crypto. Remove these Ciphers from the list and then you will have to reboot the TMS Server for the changes to take affect. It is recommended that this be done at off peak hours at the time of a maintenance window to ensure users are not affected by this change.

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