

Windows密码器在TMS和Openssl之间的原因 TLS问题根据设备

目录

[简介](#)

[背景信息](#)

[问题](#)

[解决方案](#)

简介

本文描述导致的问题，当思科网真管理套件(TMS)时无法连接到其受管理设备和那里是在思科TMS报告的“没有https答复”错误。思科TMS不能开始/管理/监视器会议。

背景信息

排除故障TMS和受管理设备之间的连接应该执行，在您尝试此解决方案前。

这些步骤应该包括：

1. 请使用在TMS服务器的捕获软件(前。)保证TMS和受管理设备之间的网络连通性的Wireshark。

2. 跟随这些技术说明：

- <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>

问题

数据包捕获的分析表明有与密码器主机TMS和思科TMS受管理设备包括会议网桥和终端的套件协商和使用方法的一个问题在Windows服务器之间。

解决方案

当用于主机TMS从Windows服务器的一传输层安全(TLS)连接的某些密码器禁用，解决了报告“受管理设备的没有https答复”错误思科TMS的一些问题。这能启用会议将正确地启动和监控。当您使用在<https://support.microsoft.com/en-us/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-november-11,-2014>时注释的详细信息，如果根据Microsoft的建议禁用这些密码器，可能缓和问题：

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

也发现也许有可能导致问题的其他密码器，当TLS连接从Windows客户端时协商。欲知更多信息，参考KB3172605问题和其解决方案从此站点：<https://social.technet.microsoft.com/Forums/en-US/ccb5a498-ab3b-441d-a854-06b5e5af3bd7/kb3172605-issues-and-solution?forum=w7itprosecurity>。当这些密码器禁用时，那使用了从主机TMS的Windows服务器的一TLS连接，它能解决“没有https答复”错误的一些问题用TMS受管理设备：

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

如何删除密码器？

简单方法从TMS服务器删除密码器将使用呼叫crypto的互联网信息服务的第三方工具(IIS)。从列表删除这些密码器您然后将必须重新启动更改的TMS服务器能采取影响。推荐这执行在非高峰时间在维护窗口时保证用户没有影响的是受此更改的。

<https://www.nartac.com/Products/IISCrypto>



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.

Schannel



Cipher Suites



Templates



Site Scanner



About

- 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