

如何在TC/CE终端升级以后排除“在TMS的没有HTTPS回应”错误故障

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[问题](#)

[解决方案](#)

[Enable \(event\)在TMS Windows服务器的TLS 1.1和1.2 TMS的15.x和更高](#)

[在TMS工具的安全性变化](#)

[考虑为了升级安全设置](#)

[Verify](#)

[对于TMS版本低于15](#)

[简介](#)

本文描述如何排除“在网真管理套件(TMS)的没有HTTPS回应”消息故障。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco TMS
- Windows 服务器

Components Used

本文档中的信息基于以下软件版本：

- TC 7.3.6以上
- CE 8.1.0以上
- TMS 15.2.1
- Windows服务器2012 R2
- SQL server 2008 R2和2012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

背景信息

此问题出现，当终端被移植到TC 7.3.6和协作终端(CE)时8.1.0软件以上。

问题

在对TC7.3.6的终端升级以上或8.1.0以上和在终端和TMS之间的通信方法设置作为传输层安全(TLS)后，错误信息“HTTPS回应”在TMS不冒出通过选择终端，根据系统>浏览器。

这发生由于此情况。

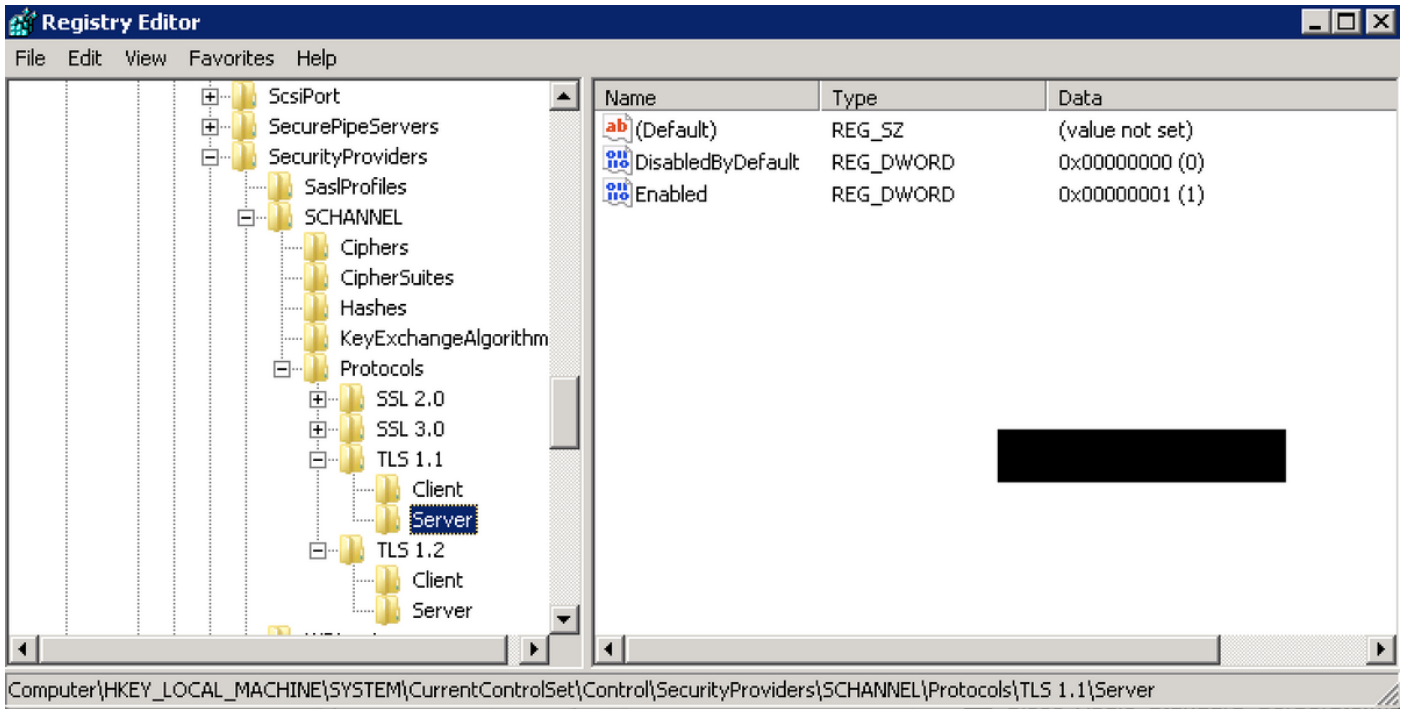
- 在不再上的TC 7.3.6和CE 8.1.0和根据版本注释支持TLS 1.0。
http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf
- 默认情况下微软视窗服务器有被禁用的TLS版本1.1和1.2。
- 默认情况下TMS工具在其传输层安全选项使用中等通信安全性。
- 当TLS版本1.0是失效的时，并且两个TLS版本1.1和1.2是启用的，TMS不发送安全套接字层SSL客户端Hello，在TCP三通的握手成功与终端后。使用TLS版本1.2，能加密数据。
- 仍然，因为TMS只将发送或通告1.0在其客户端hello消息，启用TLS版本1.2使用工具或在Windows注册表不是足够。

解决方案

TMS安装的Windows服务器，需要有被启用的TLS版本1.1和1.2，这可以用下个程序完成。

Enable (event)在TMS Windows服务器的TLS 1.1和1.2 TMS的15.x和更高

- 1.TMSWindows
- 2.Windows(Start->Run->Regedit)
3.
 -
 -
 - file
 -
 - Click **Save**.
4. Enable (event) TLS 1.1TLS 1.2
 -
 - HKEY_LOCAL_MACHINE-->SYSTEM--> CurrentControlSet--> SecurityProviders--> SCHANNEL-->**
 - TLS 1.1TLS 1.2
 - TLS 1.1TLS 1.2
 - client'



DWORDsTLS

DisabledByDefault [Value = 0]

Enabled [Value = 1]

5.TLSTMS Windows

Note:aplicablehttps://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

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

在TMS工具的安全性变化

当正确的版本是启用的时，请更改在TMS工具的安全设置有此程序的。

步骤1.打开TMS工具

步骤2.连接对**安全设置>Advanced安全设置**

第 3 步：在**传输层安全选项**下，请设置通信安全性对媒体高

步骤4.点击**“Save”**

第 5 步：然后请重新启动互联网信息服务(IIS)在服务器和TMSDatabaseScannerService并且开始TMSPLCMDirectoryService (如果终止了)

警告：:: 当TLS选项更改到媒体高从媒体， telnet和简单网络管理协议(SNMP)将是失效的。这将造成TMSSNMPservice终止，并且戒备在TMS Web接口将被上升。

考虑为了升级安全设置

当SQL 2008 R2是在使用中和在TMS Windows服务器上时安装，我们需要保证TLS1.0和SSL3.0应该也是启用的或者SQL服务必须先停止和不会开始。

您必须发现此在事件日志的错误：

Icon	Time	Source	Level	Category
Error	5/25/2016 9:31:16 PM	MSSQL\$SQLTMS	26011	Server
Error	5/25/2016 8:35:48 PM	MSSQL\$SQLTMS	3999	Server
Error	5/25/2016 7:09:29 PM	MSSQL\$SQLTMS	3999	Server
Error	5/25/2016 5:43:08 PM	MSSQL\$SQLTMS	3999	Server

Event 26011, MSSQL\$SQLTMS

General | Details

The server was unable to initialize encryption because of a problem with a security library. The security library may be missing. Verify that security.dll exists on the system.

当SQL 2012是在使用中的时要求更新处理TLS更改，如果在TMS Windows服务器(<https://support.microsoft.com/en-us/kb/3052404>)上安装

使用SNMP管理的终端或Telnet显示“破坏安全：Telnet通信不允许”。

MI-AHOC-HDX-Test2

Polycom HDX 9002 Status: Security violation: Telnet communication is not allowed Address: 10.20.65.121 Connectivity: Reachable on LAN Software version: Release - 3.1.10-51067

Edit Settings | Ticket Filters | Ticket Log

Tickets

Warning! Connection status is 'Security violation: Telnet communication is not allowed'. The settings and diagnostic messages may be unreliable.

Open:

#1160969 - TMS Connection Error (5/25/2016 9:29:19 PM)
There is a connection problem between TMS and the system.

► Add custom ticket ► Open system in System Navigator

Verify

当您从媒体更改TLS选项到媒体高时，这保证TLS版本1.2在客户端Hello做通告，在TCP三通的握手从TMS后成功：

784	19.841819	10.48.36.26	10.10.245.131	TCP	66 58930 → 443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
785	19.843295	10.10.245.131	10.48.36.26	TCP	66 443 → 58930 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=64
786	19.843340	10.48.36.26	10.10.245.131	TCP	54 58930 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
787	19.843744	10.48.36.26	10.10.245.131	TLSv1.2	351 Client Hello

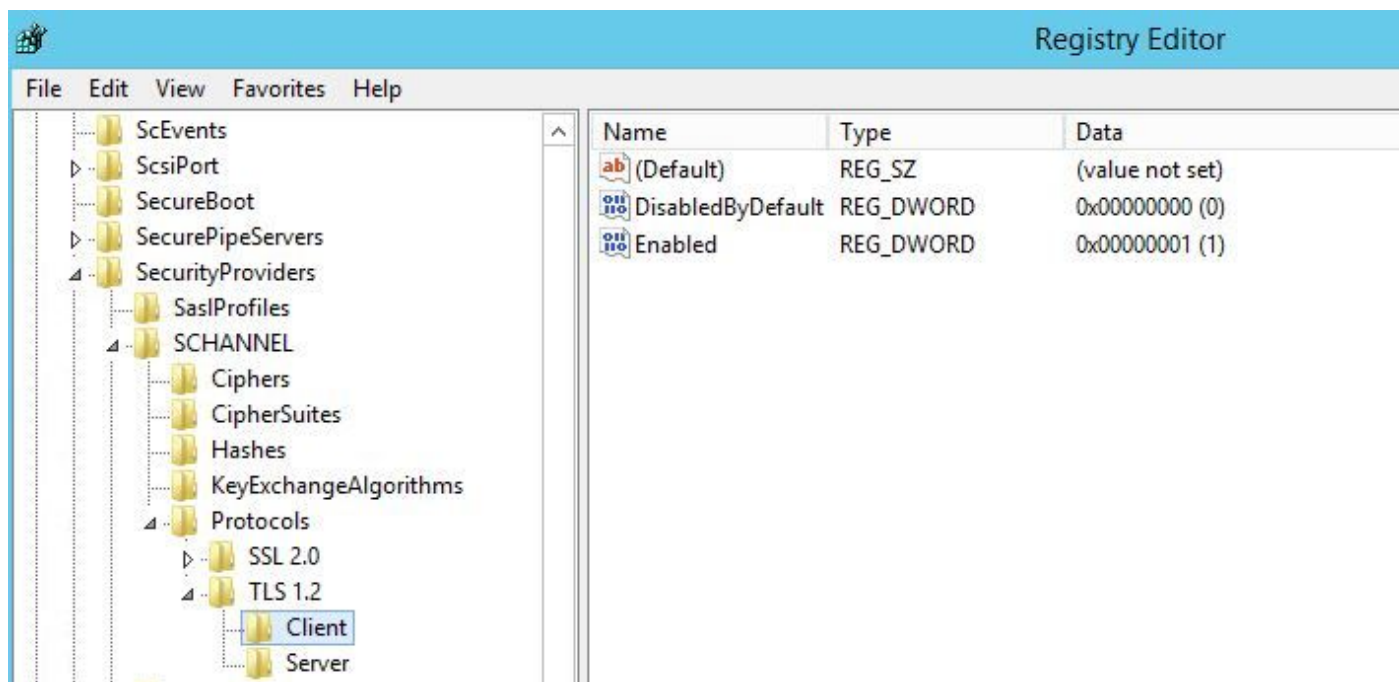
做通告的TLS版本1.2：

```
▶ Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
▶ Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
▶ Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
▶ Transmission Control Protocol, Src Port: 58930 (58930), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 297
4 Secure Sockets Layer
  4 TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 292
  ▶ Handshake Protocol: Client Hello
```

如果它离开在中等TMS只将发送在SSL客户端Hello的版本1.0在指定最高的TLS协议版本支持作为客户端，TMS是的协商阶段期间，在这种情况下。

对于TMS版本低于15

步骤1.即使TLS版本1.2在注册被添加



Step 2.TMS服务器仍然不发送在其SSL客户端Hello的终端支持的版本

1287	11.9999090	10.48.79.117	10.10.0.53	TCP	66 57380-443	[SYN, ECN, cWR] Seq=0 w
1288	12.0011950	10.10.0.53	10.48.79.117	TCP	66 443-57380	[SYN, ACK] Seq=0 Ack=1
1289	12.0012090	10.48.79.117	10.10.0.53	TCP	54 57380-443	[ACK] Seq=1 Ack=1 win=6
1290	12.0013900	10.48.79.117	10.10.0.53	SSL	157	Client Hello
1291	12.0027650	10.10.0.53	10.48.79.117	TCP	60 443-57380	[ACK] Seq=1 Ack=104 win
1292	12.0035480	10.10.0.53	10.48.79.117	TCP	60 443-57380	[RST, ACK] Seq=1 Ack=10
1294	12.0068970	10.48.79.117	10.10.0.53	TCP	66 57381-80	[SYN, ECN, cWR] Seq=0 wi
1295	12.0084020	10.10.0.53	10.48.79.117	TCP	66 80-57381	[SYN, ACK] Seq=0 Ack=1 w
1296	12.0084170	10.48.79.117	10.10.0.53	TCP	54 57381-80	[ACK] seq=1 Ack=1 win=65
1297	12.0084980	10.48.79.117	10.10.0.53	HTTP	217	GET /tcs/systemunit.xml HTTP/1.1
1298	12.0099360	10.10.0.53	10.48.79.117	TCP	60 80-57381	[ACK] Seq=1 Ack=164 win=
1299	12.0104210	10.10.0.53	10.48.79.117	HTTP	444	HTTP/1.1 301 Moved Permanently (
1300	12.0105360	10.10.0.53	10.48.79.117	TCP	60 80-57381	[FIN, ACK] Seq=391 Ack=1

Frame 1290: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
Ethernet II, Src: Vmware_99:42:e9 (00:50:56:99:42:e9), Dst: Cisco_29:96:c7 (00:1b:54:29:96:c7)
Internet Protocol Version 4, Src: 10.48.79.117 (10.48.79.117), Dst: 10.10.0.53 (10.10.0.53)
Transmission Control Protocol, Src Port: 57380 (57380), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 10
Secure Sockets Layer
SSL Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 98
Handshake Protocol: Client Hello

第 3 步：问题在事实然后在我们不能更改在TMS工具的TLS选项，因为此选项不是可用的

Encryption Key

TLS Client Certificates

Advanced Security Settings

Optional Features Control

- Disable Provisioning
- Disable SNMP

Auditing

- Auditing Always Enabled

Transport Layer Security Options

- Request Client Certificates for HTTPS API
- Enable Certificate Revocation Check

Banners

- Banners on Web Pages and Documents

Top Banner: Bottom Banner:

Restart IIS and all TMS services for the changes to take effect.

SAVE

第 4 步：然后此问题的解决方法是升级TMS到15.x或降低您的TC/CE终端到7.3.3，此问题被跟踪在版本14.6.X [CSCuz71542](#)创建的软件缺陷。