Probleemoplossing voor "geen HTTPS-respons"-fout bij TMS na upgrade op TC/CE-endpoints

Inhoud

Inleiding

In dit document wordt beschreven hoe u een "HTTPS-bericht" op TelePresence Management Suite (TMS) kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco TMS
- Windows Server

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- TC 7.3.6 en hoger
- CE 8.1.0 en hoger
- TMS 15.2.1
- Windows Server 2012 R2
- SQL Server 2008 R2 en 2012

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Dit probleem doet zich voor wanneer de endpoints worden gemigreerd naar software voor TC 7.3.6 en Collaboration-endpoint (CE) 8.1.0 of hoger.

Probleem

Na een upgrade op een eindpunt naar TC7.3.6 of hoger of 8.1.0 of hoger en de communicatiemethode tussen het eindpunt en de TMS is ingesteld als Transport Layer Security (TLS), verschijnt de foutmelding "geen HTTPS-respons" op TMS door het Endpoint te selecteren onder **System > Navigator**.

Dit is het gevolg van deze situatie.

- TC 7.3.6 en CE 8.1.0 en hoger ondersteunen TLS 1.0 niet langer, zoals in de vrijgaveaantekeningen staat. http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf

- De Microsoft Windows-server is standaard uitgeschakeld met TLS versie 1.1 en 1.2.
- TMS-tools gebruiken standaard Medium Communication Security in de transportlaag Beveiligingsopties.
- Wanneer TLS versie 1.0 wordt uitgeschakeld en beide TLS-versies 1.1 en 1.2 zijn ingeschakeld, stuurt TMS geen Secure Socket Layer (SSL) Client naar bed nadat TCP 3-way handshake met het Endpoint succesvol is. Gegevens kunnen echter nog worden versleuteld met TLS versie 1.2.
- Het is niet voldoende om TLS versie 1.2 in te schakelen met behulp van een tool of in het Windows-register, aangezien de TMS alleen 1.0 in de hallo-berichten van de client zal verzenden of bekendmaken.

Oplossing

Op de Windows server waar de TMS is geïnstalleerd, is TLS versie 1.1 en 1.2 ingeschakeld. Dit kan met de volgende procedure worden bereikt.

TLS 1.1 en 1.2 op TMS Windows Server inschakelen voor TMS 15.x en hoger

Stap 1. Open een afstandsbediening naar Windows Server waar TMS is geïnstalleerd.

Stap 2. Open Windows-editor (**Start**->**Start**->**Regedit**).

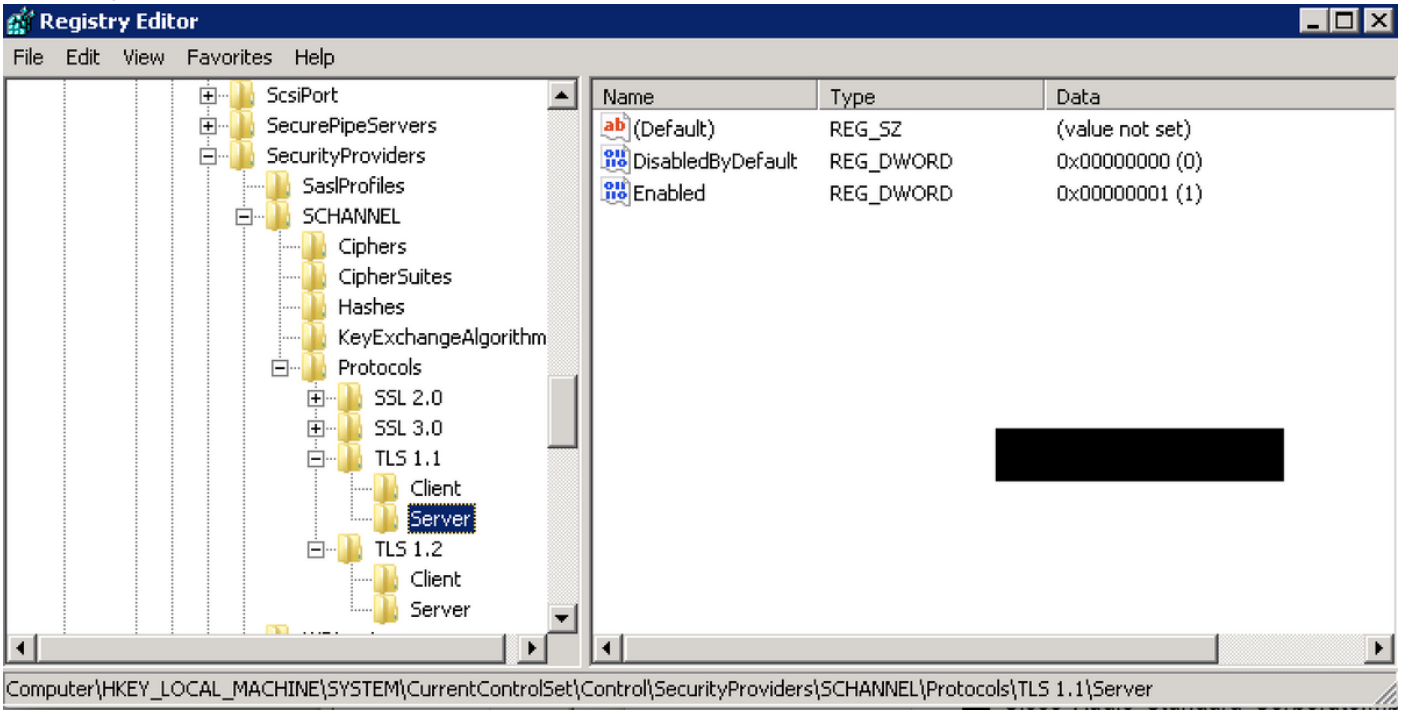
Stap 3. Neem een back-up van de griffie.

Als u om een wachtwoord of bevestiging voor een beheerder wordt gevraagd, typt u het wachtwoord of geeft u een bevestiging.
Pak de optie en klik op de toets of de subtoets waarvan u een back-up wilt maken.
Klik op het menu Bestand en vervolgens op Exporteren.
Selecteer in het vakje Opslaan in, de locatie waar u de reservekopie wilt opslaan naar, en typ vervolgens een naam voor het reservekopiebestand in het vak Bestandsnaam.
Klik op Opslaan.

Stap 4. Schakel TLS 1.1 en TLS 1.2 in.

Openbaar register
Navigeren in op **HKEY_LOCAL_MACHINE** —> **SYSTEEM** —> **Huidige ControlSet** —> **Control** —> **SeSecurity providers**—> **SCHANNEL** —> **Protocollen**
Ondersteuning van TLS 1.1 en TLS 1.2 toevoegen

TLS 1.1 en TLS 1.2 mappen maken
Subkeys als client' en 'server' maken



DWORD's maken voor zowel client- als serversoftware voor elke nieuwe TLS-toets.

```
DisabledByDefault [Value = 0]
Enabled [Value = 1]
```

Stap 5. Start de TMS Windows-server opnieuw om er zeker van te zijn dat TLS wordt uitgevoerd.

Opmerking: Bezoek deze link voor specifieke informatie over toepasbare versies https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

Tip: u kunt NARTAC-gereedschap gebruiken om de TLS-gewenste versies uit te schakelen nadat u hebt gedaan dat u de server opnieuw moet opstarten. U kunt het downloaden van deze link https://www.nartac.com/Products/IISCrypto/Download

Security verandering in TMS Tool

Als de juiste versies zijn ingeschakeld, wijzigt u de beveiligingsinstellingen op TMS-tools met deze procedure.

Stap 1. Open TMS-tools

Stap 2. Navigeer naar **beveiligingsinstellingen > Geavanceerde beveiligingsinstellingen**

Stap 3. **Stel** onder **Beveiligingsopties op transportlaag** de communicatie in op **Gemiddeld**

Stap 4. Klik op **Opslaan**

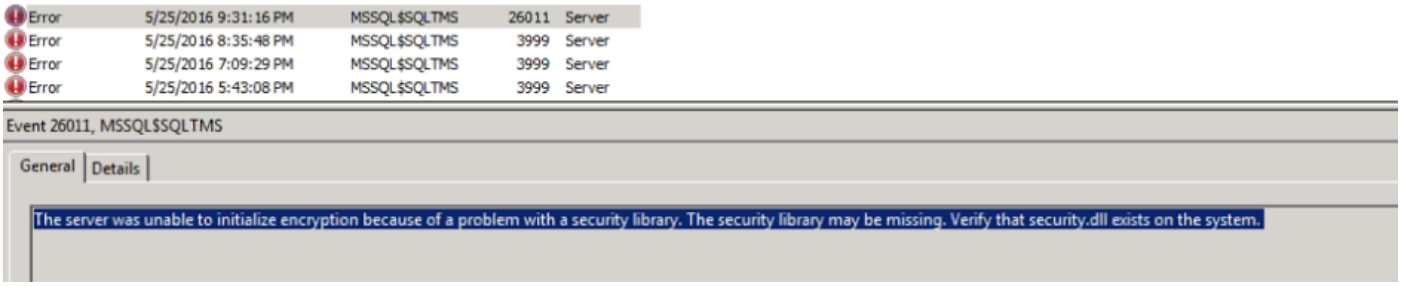
Stap 5. Start vervolgens zowel de Internet Information Services (IS) op de server als **TMSDatabaseScannerService** opnieuw en start **TMSPLCMD**Director **Service** (indien deze is gestopt)

Waarschuwing: : Wanneer TLS-optie wordt gewijzigd in Medium-High vanuit Medium, worden telnet en Simple Network Management Protocol (SNMP) uitgeschakeld. Dit zal ervoor zorgen dat de TMSSNMP-service stopt en er zal een waarschuwing worden opgevoerd op de TMS-web interface.

Overdenkingen voor het upgraden van beveiligingsinstellingen

Wanneer **SQL 2008 R2** in gebruik is en op TMS windows server is geïnstalleerd, moeten we er zeker van zijn dat TLS1.0 en SSL3.0 ook ingeschakeld zijn of anders SQL service stop en het start niet.

U moet deze fouten in het logbestand van de gebeurtenis zien:

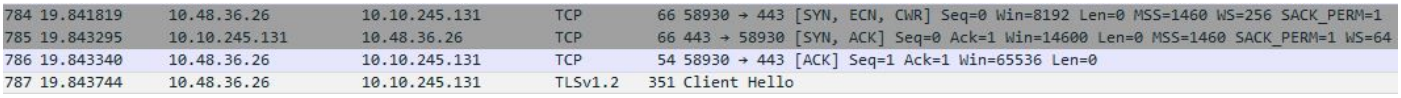


Wanneer **SQL 2012** in gebruik is, moet deze worden bijgewerkt om TLS-verandering aan te pakken indien geïnstalleerd op TMS windows server (https://support.microsoft.com/en-us/kb/3052404)

Endpoints die worden beheerd met behulp van SNMP of telnet tonen "Veiligheidsschending: Telnet-communicatie is niet toegestaan".

Verifiëren

Wanneer u de TLS-optie van **Gemiddeld** naar **Gemiddeld-Hoog** verandert**,** zorgt dit ervoor dat TLS versie 1.2 geadverteerd wordt in de **Client Hallo** nadat de TCP 3-way handdruk van TMS is bereikt:



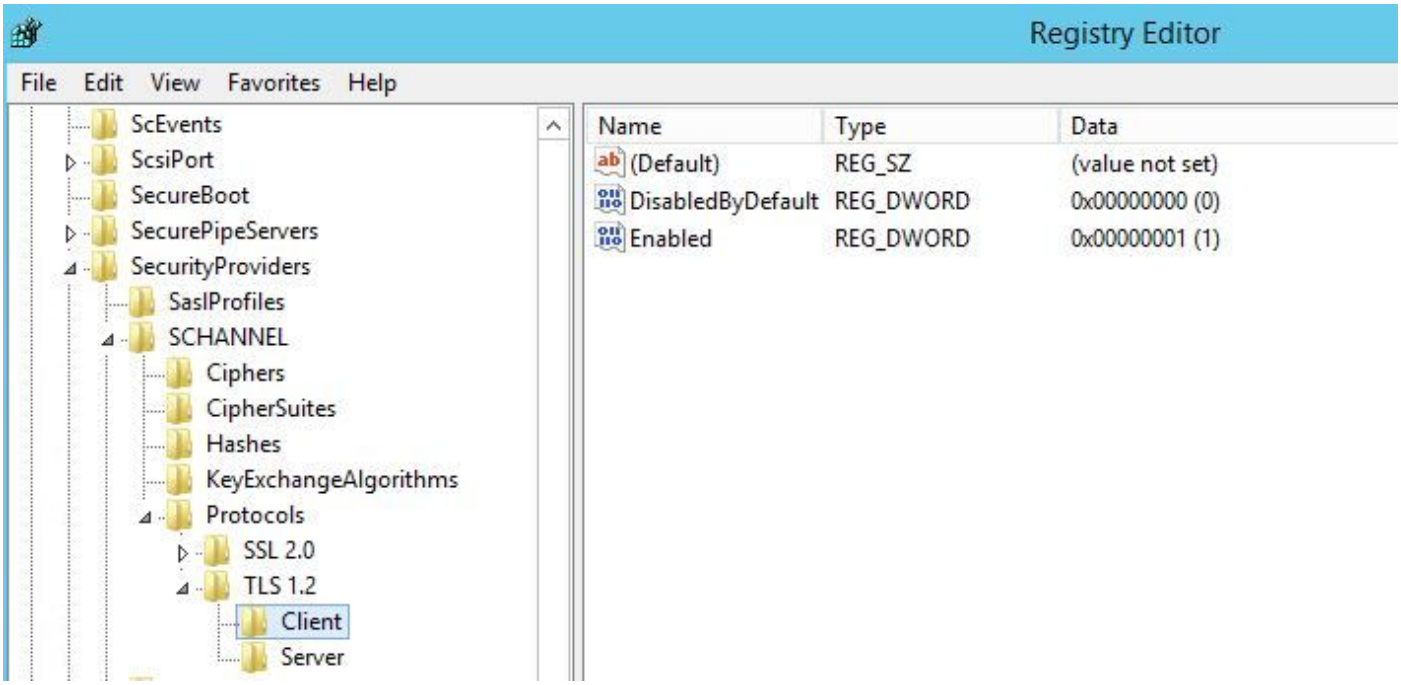
Aanbevolen TLS versie 1.2:

```
▷ 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
◢ Secure Sockets Layer
  ◢ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 292
    ▷ Handshake Protocol: Client Hello
```

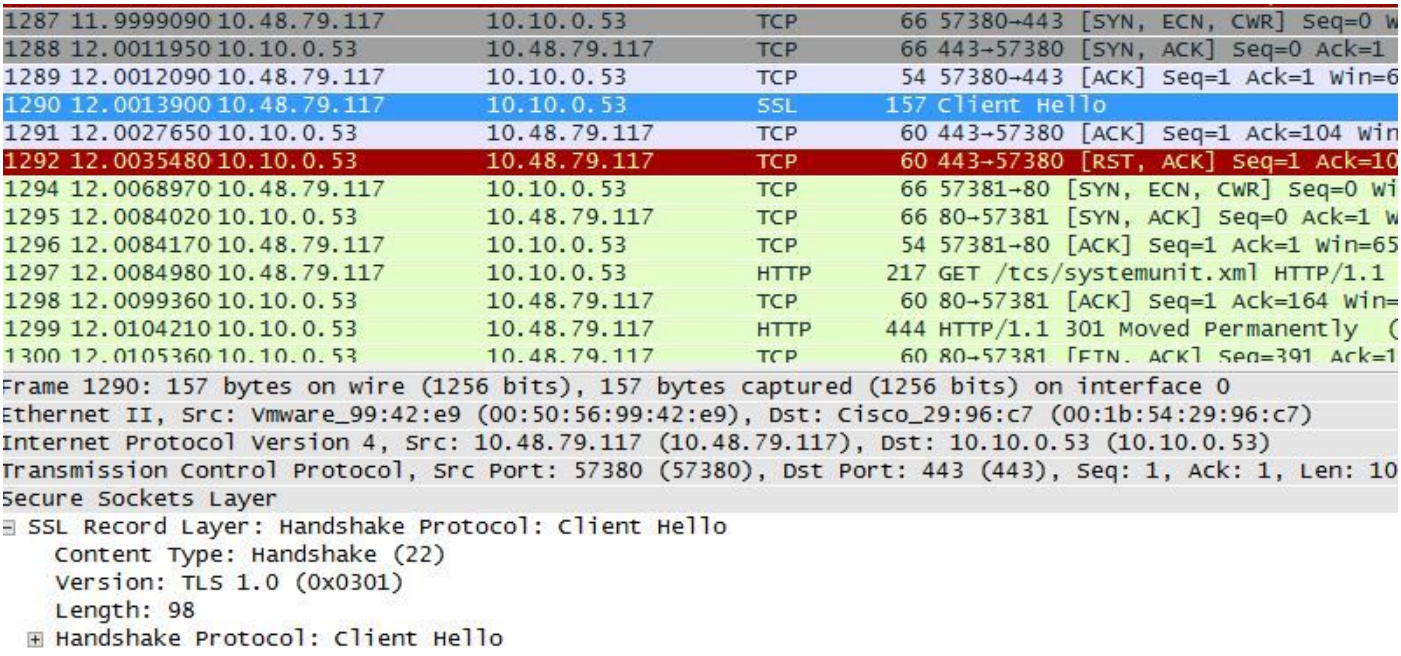
Als deze optie op **medium** TMS is achtergelaten, wordt versie 1.0 in de SSL-client alleen tijdens de onderhandelingsfase verzonden. In deze fase wordt de hoogste TLS-protocolversie gespecificeerd die de client ondersteunt als client, wat TMS in dit geval is.

Voor TMS-versies onder de 15

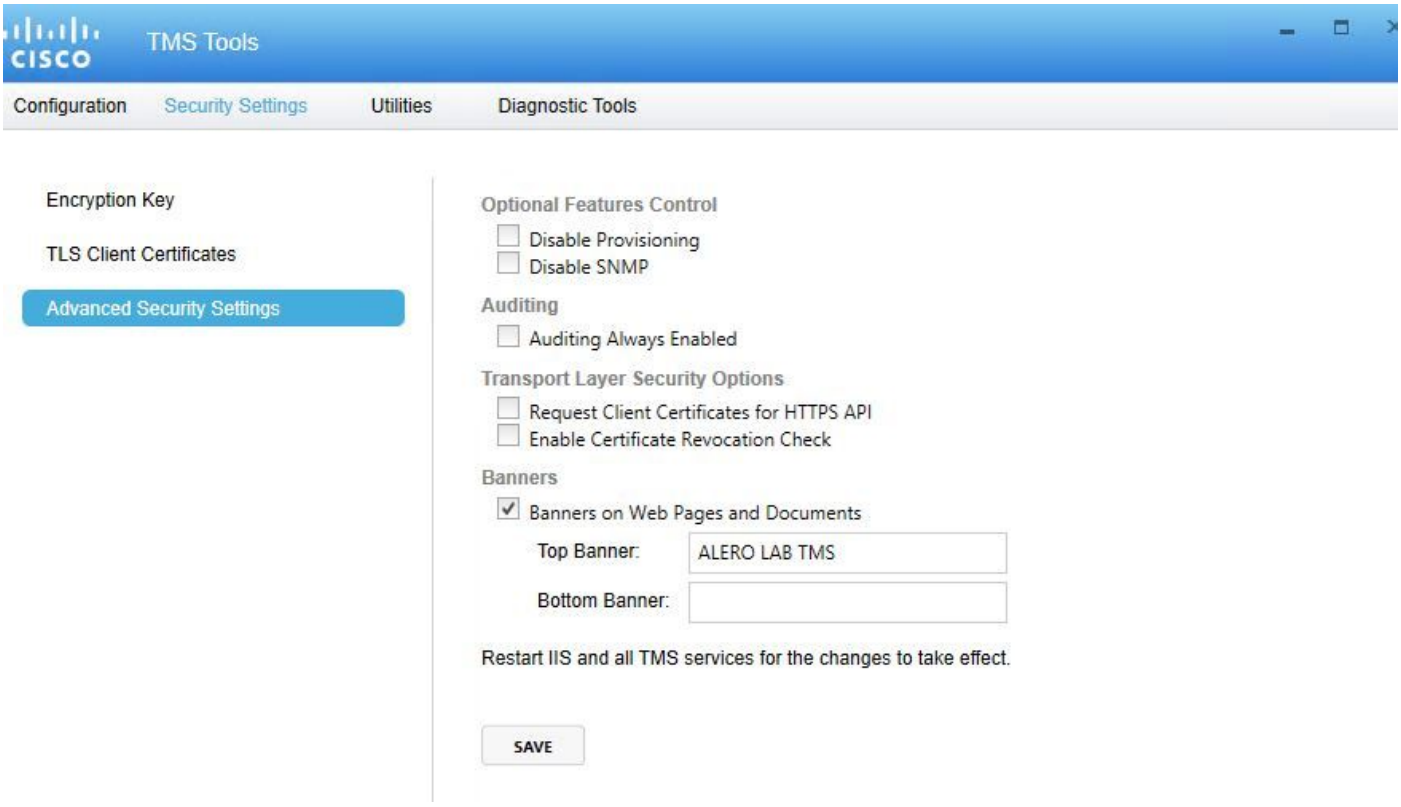
Stap 1. Ook al wordt versie 1.2 van het TLS in het register toegevoegd



Stap 2. De TMS-server stuurt nog steeds niet de versie die wordt ondersteund door Endpoint in de SSL-client



Stap 3. Het probleem is dan dat we de TLS-opties in TMS-tools niet kunnen wijzigen omdat deze optie niet beschikbaar is



Stap 4. Vervolgens is het tijdelijke probleem voor deze kwestie of het upgraden van TMS naar 15.x of het downloaden van uw TC/CE-eindpunten naar 7.3.3. Dit probleem wordt opgelost in softwaredefect CSCuz71542 dat is gemaakt voor versie 14.6.X.