

Desative o TLS 1.1 nos Switches Catalyst 9000

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Passo 1: Verifique a presença do TLS 1.1](#)

[Solução](#)

[Passo 1: Desabilitar TLS 1.1 para Servidor HTTP](#)

[Passo 2: Desabilitar TLS 1.1 para Cliente HTTP](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como desativar o Transport Layer Security(TLS) 1.1 nos switches Catalyst 9000 em redes LAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos de LAN switching
- Navegação básica na interface de linha de comando (CLI)
- Compreensão dos protocolos TLS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9000 Series Switch
- Versão de software: 17.6.5

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento fornece um guia técnico para localizar e desativar o TLS 1.1 nos switches Catalyst 9000.

Problema

O problema envolve a detecção de TLS 1.1 no switch. Isso é sinalizado para várias varreduras antivulnerabilidades,

Passo 1: Verifique a presença do TLS 1.1

<#root>

Switch#

show ip http server secure status

```
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite:  rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
                                dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
                                ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2 tls13-aes128-gcm-sha256
                                tls13-aes256-gcm-sha384 tls13-chacha20-poly1305-sha256
```

HTTP secure server TLS version:

TLSv1.3 TLSv1.2

TLSv1.1 <<< Presense of TLSv1.1 in the HTTP Server

```
HTTP secure server client authentication: Disabled
HTTP secure server PIV authentication: Disabled
HTTP secure server PIV authorization only: Disabled
HTTP secure server trustpoint: TP-self-signed-3889524895
HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL
```

Switch#

show ip http client secure status

```
HTTP secure client ciphersuite:  rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
                                dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
                                ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2 tls13-aes128-gcm-sha256
                                tls13-aes256-gcm-sha384 tls13-chacha20-poly1305-sha256
```

HTTP secure client TLS version:

TLSv1.3 TLSv1.2

TLSv1.1 <<< Presence of TLSv1.1 in the HTTP client

HTTP secure client trustpoint:

Solução

Siga estas etapas para desativar o TLS 1.1 em switches Catalyst 9000:

Passo 1: Desabilitar TLS 1.1 para Servidor HTTP

```
<#root>
```

```
Switch#
```

```
configure terminal
```

```
Switch(config)#
```

```
no ip http tls-version TLSv1.1
```

Passo 2: Desabilitar TLS 1.1 para Cliente HTTP

```
<#root>
```

```
Switch#
```

```
configure terminal
```

```
Switch(config)#
```

```
no ip http client tls-version TLSv1.1
```

Esses comandos garantem que o TLS 1.1 seja desativado nos lados do servidor e do cliente do switch, minimizando quaisquer preocupações de segurança associadas a protocolos desatualizados.

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.