在Catalyst 9000交换机上禁用TLS 1.1

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[问题](#)

[步骤 1：检验TLS 1.1是否存在](#)

[解决方案](#)

[步骤 1：为HTTP服务器禁用TLS 1.1](#)

[步骤 2：为HTTP客户端禁用TLS 1.1](#)

[相关信息](#)

简介

本文档介绍如何在LAN网络中的Catalyst 9000交换机上禁用传输层安全(TLS)1.1。

先决条件

要求

Cisco 建议您了解以下主题：

- LAN交换概念
- 基本命令行界面(CLI)导航
- 了解TLS协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 9000 系列交换机
- 软件版本:17.6.5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档提供了在Catalyst 9000交换机上查找和禁用TLS 1.1的技术指南。

问题

问题涉及在交换机上检测到TLS 1.1。此标记用于多个防漏洞扫描，

步骤 1：检验TLS 1.1是否存在

```
<#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                <<< Presence 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:
```

解决方案

执行以下步骤在Catalyst 9000交换机上禁用TLS 1.1:

步骤 1：为HTTP服务器禁用TLS 1.1

```
<#root>
```

```
Switch#
```

```
configure terminal
```

```
Switch(config)#
```

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

步骤 2：为HTTP客户端禁用TLS 1.1

```
<#root>
```

```
Switch#
```

```
configure terminal
```

```
Switch(config)#
```

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

这些命令可以确保在交换机的服务器和客户端上都禁用TLS 1.1，从而缓解与过时协议相关的任何安全问题。

相关信息

- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。