在Catalyst 9000交換機上禁用TLS 1.1

目錄

簡介

本文說明如何在LAN網路的Catalyst 9000交換器上停用傳輸層安全(TLS)1.1。

必要條件

需求

思科建議您瞭解以下主題：

- LAN交換概念
- 基本命令列介面(CLI)導航
- 瞭解TLS協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9000系列交換器
- 軟體版本:17.6.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔提供了在Catalyst 9000交換機上查詢和禁用TLS 1.1的技術指南。

問題

問題涉及在交換機上檢測到TLS 1.1。此標籤用於多個防漏洞掃描，

步驟 1:驗證TLS 1.1的存在

<#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                    <<< 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:
```

解決方案

執行以下步驟在Catalyst 9000交換機上禁用TLS 1.1:

步驟 1:為HTTP伺服器禁用TLS 1.1

<#root>

Switch#

configure terminal

Switch(config)#

no ip http tls-version TLSv1.1

步驟 2:為HTTP客戶端禁用TLS 1.1

<#root>

Switch#

configure terminal

Switch(config)#

no ip http client tls-version TLSv1.1

這些命令可確保TLS 1.1在交換機的伺服器和客戶端上均被禁用，從而減輕與過期協定相關的任何安全問題。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。