Catalyst 9000 스위치에서 TLS 1.1 비활성화

목차

소개

이 문서에서는 LAN 네트워크의 Catalyst 9000 스위치에서 TLS(Transport Layer Security) 1.1을 비활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LAN 스위칭 개념
- 기본 CLI(Command Line Interface) 탐색
- TLS 프로토콜에 대한 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9000 Series 스위치
- 소프트웨어 버전: 17.6.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 Catalyst 9000 스위치에서 TLS 1.1을 찾고 비활성화하는 방법에 대한 기술 가이드를 제공합니다.

문제

이 문제는 스위치에서 TLS 1.1이 탐지되는 것과 관련이 있습니다. 여러 개의 안티취약성 스캔에 대해 플래그가 지정됩니다.

1단계: TLS 1.1의 존재 확인

<#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:
```

솔루션

Catalyst 9000 스위치에서 TLS 1.1을 비활성화하려면 다음 단계를 수행하십시오.

1단계: HTTP 서버에 대해 TLS 1.1 비활성화

<#root>

```
Switch#
configure terminal

Switch(config)#
no ip http tls-version TLSv1.1
```

2단계: HTTP 클라이언트에 대해 TLS 1.1 비활성화

<#root>

```
Switch#
configure terminal

Switch(config)#
no ip http client tls-version TLSv1.1
```

이 명령을 사용하면 스위치의 서버 및 클라이언트 측에서 모두 TLS 1.1이 비활성화되어 오래된 프로토콜과 관련된 보안 문제를 완화할 수 있습니다.

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.