Catalyst 9000スイッチ上のTLS 1.1の無効化

内容

はじめに

このドキュメントでは、LANネットワークのCatalyst 9000スイッチでTransport Layer Security(TLS)1.1を無効にする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- LANスイッチングの概念
- 基本的なコマンドラインインターフェイス(CLI)ナビゲーション
- TLSプロトコルの理解

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9000 シリーズ スイッチ
- ソフトウェアバージョン：17.6.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、Catalyst 9000スイッチでTLS 1.1を見つけて無効にするためのテクニカルガイドを提供します。

問題

この問題には、スイッチでのTLS 1.1の検出が含まれます。複数の脆弱性スキャンのフラグが付けられます

ステップ1:TLS 1.1の存在の確認

<#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:
```

解決方法

Catalyst 9000スイッチでTLS 1.1を無効にするには、次の手順を実行します。

ステップ1:HTTPサーバのTLS 1.1を無効にする

<#root>

Switch#

configure terminal

Switch(config)#

no ip http tls-version TLSv1.1

ステップ2:HTTPクライアントのTLS 1.1を無効にする

<#root>

Switch#

configure terminal

Switch(config)#

no ip http client tls-version TLSv1.1

これらのコマンドにより、スイッチのサーバ側とクライアント側の両方でTLS 1.1が無効になり、古いプロトコルに関連するセキュリティ上の問題が軽減されます。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。