Disable TLS 1.1 on Catalyst 9000 Switches

Contents

Introduction

This document describes how to disable Transport Layer Security(TLS) 1.1 on Catalyst 9000 switches in LAN networks.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- LAN switching concepts
- Basic command line interface (CLI) navigation
- Understanding of TLS protocols

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 9000 Series Switch
- Software Version: 17.6.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document provides a technical guide for locating and disabling TLS 1.1 on Catalyst 9000 switches.

Problem

The problem involves TLS 1.1 being detected on the switch. This is flagged for several anti vulnerabilities scan,

Step 1: Verify the Presence of 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:
```

Solution

Take these steps to disable TLS 1.1 on a Catalyst 9000 switches:

Step 1: Disable TLS 1.1 for HTTP Server

<#root>

```
Switch#

configure terminal

Switch(config)#

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

Step 2: Disable TLS 1.1 for HTTP Client

<#root>

```
Switch#

configure terminal

Switch(config)#

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

These commands ensure that TLS 1.1 is disabled on both the server and client sides of the switch, mitigating any security concerns associated with outdated protocols.

Related Information

- Cisco Technical Support & Downloads