Deaktivieren von TLS 1.1 auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Transport Layer Security (TLS) 1.1 auf Catalyst 9000-Switches in LAN-Netzwerken deaktiviert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- LAN-Switching-Konzepte
- Einfache Navigation über die Kommandozeile (CLI)
- Verständnis von TLS-Protokollen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst Switches der Serie 9000
- Software-Version: 17.6.5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Dokument enthält einen technischen Leitfaden für die Suche nach und Deaktivierung von TLS 1.1 auf Catalyst 9000-Switches.

Problem

Das Problem besteht darin, dass TLS 1.1 auf dem Switch erkannt wird. Dies wird für mehrere Anti-Schwachstellen-Scans markiert,

Schritt 1: Überprüfen des Vorhandenseins von 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:
```

Lösung

Gehen Sie folgendermaßen vor, um TLS 1.1 auf einem Catalyst 9000-Switch zu deaktivieren:

Schritt 1: TLS 1.1 für HTTP-Server deaktivieren

<#root>

```
Switch#
configure terminal

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

Phase 2: TLS 1.1 für HTTP-Client deaktivieren

<#root>

```
Switch#
configure terminal

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

Diese Befehle stellen sicher, dass TLS 1.1 sowohl auf der Server- als auch auf der Clientseite des Switches deaktiviert ist, sodass alle Sicherheitsbedenken im Zusammenhang mit veralteten Protokollen ausgeräumt werden.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.