Disabilitazione di TLS 1.1 sugli switch Catalyst 9000

Sommario

Introduzione

In questo documento viene descritto come disabilitare Transport Layer Security(TLS) 1.1 sugli switch Catalyst 9000 nelle reti LAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nozioni base sullo switching LAN
- Navigazione di base con interfaccia a riga di comando (CLI)
- Informazioni sui protocolli TLS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst serie 9000 Switch
- Versione del software: 17.6.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento offre una guida tecnica per l'individuazione e la disattivazione di TLS 1.1 sugli switch Catalyst 9000.

Problema

Il problema prevede il rilevamento di TLS 1.1 sullo switch. Questo è contrassegnato per diverse analisi anti vulnerabilità,

Passaggio 1: Verifica della presenza di 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:
```

Soluzione

Per disabilitare TLS 1.1 su uno switch Catalyst 9000, attenersi alla seguente procedura:

Passaggio 1: Disabilita TLS 1.1 per il server HTTP

<#root>

```
Switch#
configure terminal

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

Passaggio 2: Disabilita TLS 1.1 per il client HTTP

<#root>

```
Switch#
configure terminal

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

Questi comandi garantiscono che TLS 1.1 sia disabilitato sul lato server e sul lato client dello switch, riducendo i problemi di sicurezza associati ai protocolli obsoleti.

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).