Risoluzione dei problemi di autenticazione SSH sull'appliance ASA con RADIUS con password temporanea

Sommario

Problema

L'accesso SSH (Secure Shell) al software ASA (Adaptive Security Appliance) con RADIUS (Remote Authentication Dial-In User Service) e OTP (One-Time Password) non riesce quando lo stack Cisco SSH è abilitato.

Vengono generati i seguenti messaggi syslog:

```
Nov 14 2025 16:28:35: %ASA-6-113010: AAA challenge received for user from server .
Nov 14 2025 16:28:35: %ASA-4-109033: Authentication failed for admin user from . Interactive challenge
```

Ambiente

I sintomi sono osservati quando tutte le condizioni corrispondono:

- Secure Firewall 1230 con ASA in modalità single o multicontext. Il problema riguarda anche altre piattaforme hardware.
- Il server RADIUS viene utilizzato per l'autenticazione SSH:

<#root>

```
device#
```

show run | i aaa

```
aaa-server RAD-OTP protocol radius
aaa-server RAD-OTP (management) host 192.0.2.1
aaa-server RAD-OTP (management) host 192.0.2.2
aaa authentication ssh console RAD-OTP
```

- Il server RADIUS richiede e richiede un codice OTP valido o una richiesta di verifica per la corretta autenticazione.
- Lo stack Cisco SSH è abilitato sull'appliance ASA.
- Nelle versioni 9.19.1 e successive, lo stack Cisco SSH è abilitato per impostazione predefinita e può essere disabilitato facoltativamente con il comando no ssh stack cisco. Utilizzare il comando show ssh per verificare:

<#root>

```
device#

show ssh


ssh secure copy : ENABLED

ciscoSSH stack : DISABLED
```

- Nelle versioni 9.23.1 e successive questo stack non può essere disabilitato o verificato.

Risoluzione

I sintomi vengono riprodotti con successo nel laboratorio interno e tracciati nell'ID bug Cisco CSCwt57790.

Utilizzare una delle seguenti opzioni di soluzione nelle versioni interessate:

- Usare l'autenticazione locale per le connessioni SSH.
- Sul server RADIUS, disabilitare il requisito OTP per l'appliance ASA.
- Nelle versioni precedenti alla 9.23, disabilitare lo stack Cisco SSH usando il comando no ssh stack cisco. Esaminare la guida di riferimento dei comandi, i comandi e i comandi S di Cisco

Secure Firewall serie ASA e valutare il potenziale impatto della disabilitazione dello stack Cisco SSH.

Causa

La causa dell'errore di autenticazione è l'ID bug Cisco CSCwt57790.

Contenuto correlato

- ID bug Cisco CSCwi04513
- ID bug Cisco CSCwt57790
- Guida di riferimento ai comandi di Cisco Secure Firewall serie ASA, comandi S

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).