Resolución de Problemas de Falla de Autenticación SSH en ASA con RADIUS Usando una Contraseña Única

Contenido

Problema

El acceso de Secure Shell (SSH) al software Adaptive Security Appliance (ASA) con el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) mediante contraseña de un solo uso (OTP) falla cuando la pila CiscoSSH está activada.

Se generan estos mensajes de 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
```

Entorno

Los síntomas se observan cuando todas las condiciones coinciden:

- Secure Firewall 1230 con ASA en modo único o multicontexto. Otras plataformas de hardware también se ven afectadas.
- El servidor RADIUS se utiliza para la autenticación 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
```

- El servidor RADIUS solicita y requiere un código OTP válido o un desafío para una autenticación correcta.
- La pila CiscoSSH está habilitada en ASA.
- En las versiones 9.19.1 y posteriores, la pila CiscoSSH se habilita de forma predeterminada y se puede inhabilitar opcionalmente mediante el comando no ssh stack cisco. Utilice el comando show ssh para la verificación:

<#root>

```
device#

show ssh


ssh secure copy : ENABLED

ciscoSSH stack : DISABLED
```

- En las versiones 9.23.1 y posteriores, esta pila no se puede deshabilitar ni verificar.

Resolución

Los síntomas se reproducen correctamente en el laboratorio interno y se realiza un seguimiento en el Id. de error de Cisco CSCwt5790.

Utilice una de estas opciones de solución alternativa en las versiones afectadas:

- Utilice la autenticación local para las conexiones SSH.
- En el servidor RADIUS inhabilite el requisito OTP para ASA.
- En versiones anteriores a la 9.23, inhabilite la pila CiscoSSH usando el comando no ssh stack cisco. Asegúrese de revisar la Referencia de Comandos, Comandos S de la Serie

ASA de Cisco Secure Firewall y evalúe el impacto potencial de desactivar la pila CiscoSSH.

Causa

La causa de la falla de autenticación es el Id. de bug Cisco CSCwt57790.

Contenido relacionado

- ID de bug de Cisco CSCwi04513
- ID de bug de Cisco CSCwt57790
- Referencia de Comandos de la Serie ASA de Cisco Secure Firewall, Comandos S

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).