使用一次性密碼對具有RADIUS的ASA上的SSH身份驗證失敗進行故障排除

目錄

問題

啟用CiscoSSH堆疊後，安全殼層(SSH)對採用一次性密碼(OTP)的遠端驗證撥入使用者服務(RADIUS)的調適型安全裝置(ASA)軟體的存取失敗。

將生成以下系統日誌消息：

```
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
```

環境

當所有條件都匹配時，將觀察以下症狀：

- 在單情景或多情景模式下使用ASA的安全防火牆1230。其他硬體平台也受到影響。
- RADIUS伺服器用於SSH驗證：

<#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
```

- RADIUS伺服器要求且需要有效的OTP代碼或詢問才能成功進行驗證。
- ASA上啟用了CiscoSSH堆疊。
- 在9.19.1及更高版本中，CiscoSSH堆疊預設處於啟用狀態，並可選擇使用no ssh stack cisco命令禁用。使用show ssh命令進行驗證:

<#root>

device#

show ssh

ssh secure copy : ENABLED

ciscoSSH stack : DISABLED

- 在9.23.1及更新版本中，無法停用或驗證此堆疊。

解析

這些症狀已成功在內部實驗室中重現並在Cisco錯誤ID CSCwt57790中跟蹤。

在受影響的版本中使用以下解決方法選項之一：

- 對SSH連線使用本地身份驗證。
- 在RADIUS伺服器上，禁用ASA的OTP要求。
- 在9.23之前的版本中，使用no ssh stack cisco 命令禁用CiscoSSH堆疊。確保檢視Cisco Secure Firewall ASA Series Command Reference， S Commands，並評估禁用CiscoSSH堆疊的潛在影響。

原因

驗證失敗的原因在於思科錯誤ID CSCwt57790。

相關內容

- 思科錯誤ID CSCwi04513
- 思科錯誤ID CSCwt57790
- 思科安全防火牆ASA系列命令參考，S命令

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。