無法使用"；未找到匹配的密碼"；通過SSH連線到Nexus 9000；收到錯誤

目錄

簡介

本文描述如何在代碼升級後對Nexus 9000的SSH問題進行故障排除/解決。

背景

在解釋SSH問題的原因之前，必須瞭解影響Nexus 9000平台的「已啟用SSH伺服器CBC模式密碼和SSH弱項MAC演算法已啟用」漏洞。

CVE ID - CVE- 2008-5161（啟用SSH伺服器CBC模式密碼和啟用SSH弱MAC演算法）

問題描述 — SSH伺服器CBC模式密碼啟用漏洞（SSH伺服器CBC模式密碼啟用）

SSH伺服器配置為支援密碼塊連結(CBC)加密。這使得攻擊者能夠從密文恢復明文消息。請注意，此外掛僅檢查SSH伺服器的選項，而不檢查是否存在易受攻擊的軟體版本。

建議的解決方案 — 禁用CBC模式密碼加密，並啟用計數器(CTR)模式或Galois/計數器模式(GCM)密碼模式加密

參考 — [國家漏洞資料庫 — CVE-2008-5161詳細資訊](#)

問題

將代碼升級到7.0(3)I2(1)後，您將無法通過SSH連線到Nexus 9000並收到以下錯誤：

```
no matching cipher found: client aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,rijndael-
cbc@lysator.liu.se server
 aes128-ctr,aes192-ctr,aes256-ctr
```

解決方案

升級到代碼7.0(3)I2(1)和更新版本後，無法通過SSH連線到Nexus 9000的原因是，弱密碼已通過Cisco錯誤ID CSCuv39937修復程式禁用。

此問題的長期解決方案是使用已禁用舊弱密碼的更新/最新SSH客戶端。

臨時解決方案是在Nexus 9000上新增弱密碼。臨時解決方案有兩種可能的選項，具體取決於代碼的版本。

臨時選項1. ssh cipher-mode weak命令(隨NXOS 7.0(3)I4(6)或更高版本提供)

- 由Cisco錯誤ID CSCvc71792引入 — 實作一個可允許弱密碼的旋鈕aes128-cbc、aes192-cbc、aes256-cbc。
- 新增對這些弱密碼的支援 — aes128-cbc、aes192-cbc和aes256-cbc。
- 仍然不**支援**3des-cbc密碼。

```
! baseline: only strong Ciphers aes128-ctr,aes192-ctr,aes256-ctrallowed
9k# conf t
Enter configuration commands, one per line. End with CNTL/Z.
9k(config)# feature bash
9k(config)# run bash sudo grep -i cipher /isan/etc/dcos_sshd_config
#secure ciphers and MACs
#CSCun41202 : Disable weaker Ciphers and MACs
Ciphers aes128-ctr,aes192-ctr,aes256-ctr    <<-----  only strong ciphers

! enable the weak aes-cbc ciphers with NXOS command
! Note that weak cipher 3des-cbc is still disabled.

9k# conf t
Enter configuration commands, one per line. End with CNTL/Z.
9k(config)# ssh cipher-mode weak
9k(config)# end

!! verification:
9k# run bash sudo grep -i cipher /isan/etc/dcos_sshd_config
#secure ciphers and MACs
#CSCun41202 : Disable weaker Ciphers and MACs
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc  <<---

! rollback: use the 'no' form of the command
9k# conf t
Enter configuration commands, one per line. End with CNTL/Z.
9k(config)# no ssh cipher-mode weak
9k(config)# end
```

臨時選項2.使用Bash修改sshd_config檔案並顯式重新新增弱密碼

如果從/isan/etc/sshd_config檔案中註釋掉密碼行，則支援所有預設密碼(包括aes128-cbc、**3des-cbc**、aes192-cbc和aes256-cbc)。

```
n9k#Config t
n9k(config)#feature bash-shell
n9k(config)#Run bash
bash-4.2$ sudo su -
root@N9K-1#cd /isan/etc
root@N9K-1#cat dcos_sshd_config | egrep Cipher
#CSCun41202 : Disable weaker Ciphers and MACs
Ciphers aes128-ctr,aes192-ctr,aes256-ctr <<<< only allowed ciphers (eliminate known
vulnerability).

!! Create a back up of the existing SSHD_CONFIG
```

```
root@N9K-1#mv dcos_sshd_config dcos_sshd_config.backup

!! comment out the cipher line and save to config (effectively removing the restriction)
cat dcos_sshd_config.backup | sed 's@^Cipher@# Cipher@g' > dcos_sshd_config
!! Verify
root@N9K-1#cat dcos_sshd_config | egrep Cipher
#CSCun41202 : Disable weaker Ciphers and MACs
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr << see inserted comment # before Cipher (to remove
the limitation)

root@N9K-1#exit
logout
bash-4.2$ exit
exit
N9K-1(config)# no feature bash
N9K-1(config)# exit
```

請注意，重新新增舊密碼後，將恢復使用弱密碼，因此存在安全風險。

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）。