无法使用"；未找到匹配的密码"；通过SSH连接到Nexus 9000；收到错误

目录

简介

本文档介绍如何在代码升级后排除/解决Nexus 9000的SSH问题。

背景

在解释SSH问题的原因之前，必须了解影响Nexus 9000平台的“已启用SSH服务器CBC模式密码和已启用SSH弱项MAC算法”漏洞。

CVE ID - CVE- 2008-5161（启用SSH服务器CBC模式密码并启用SSH弱MAC算法）

问题描述 — SSH服务器CBC模式密码已启用漏洞（SSH服务器CBC模式密码已启用）

SSH服务器配置为支持密码块链接(CBC)加密。这使得攻击者能够从密文恢复明文消息。请注意，此插件仅检查SSH服务器的选项，而不检查是否存在有漏洞的软件版本。

建议的解决方案 — 禁用CBC模式加密并启用计数器(CTR)模式或格洛瓦/计数器模式(GCM)加密模式

参考 — [国家漏洞数据库 — CVE-2008-5161详细信息](#)

问题

将代码升级到7.0(3)I2(1)后，您将无法通过SSH连接到Nexus 9000并收到以下错误：

```
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
```

解决方案

在升级到代码7.0(3)I2(1)及更高版本后，您无法通过SSH连接到Nexus 9000的原因是，弱密码通过Cisco Bug ID [CSCuv3937修复程序禁](#)用。

此问题的长期解决方案是使用已禁用旧弱密码的更新/最新SSH客户端。

临时解决方案是在Nexus 9000上重新添加弱密码。临时解决方案有两种可能的选项，具体取决于代码版本。

临时选项1. ssh cipher-mode weak命令(适用于NXOS 7.0(3)I4(6)或更高版本)

- 由Cisco Bug ID CSCvc71792引入 — 实施用于允许弱密码aes128-cbc、aes192-cbc、aes256-cbc的命令。
- 添加对这些弱密码的支持 — aes128-cbc、aes192-cbc和aes256-cbc。
- 仍然不**支持**3des-cbc密码。

```
! 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
```

临时选项2。使用Bash修改sshd_config文件并显式重新添加弱密码

如果从/isan/etc/sshd_config文件中注释掉密码行，则支持所有默认密码(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
```

请注意，重新添加旧密码后，将恢复使用弱密码，因此存在安全风险。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。