无法对SSH到连结9000用“没有匹配的密码器查找”错误接收

目录

简介

本文描述如何排除故障/在代码升级以后解决对连结9000的SSH问题。

在SSH的原因前问题解释，知道关于‘SSH服务器CBC模式加密影响连结9000平台的已启用& SSH弱MAC算法启用的’漏洞是必要的。

CVE ID - CVE- 2008-5161 (SSH服务器CBC模式加密启用的已启用& SSH弱MAC算法)

问题说明- SSH服务器CBC模式密码器已启用漏洞(SSH服务器CBC启用的模式密码器)

SSH服务器配置支持密码链块(CBC)加密。这也许允许攻击者从密文恢复明文消息。注意此插件只检查SSH服务器的选项，并且不检查易受攻击软件版本。

推荐的解决方案-禁用CBC模式密码器加密和Enable计数器(CTR)模式或者Galois/计数器模式(GCM)密码器模式加密

参考-国家漏洞数据库- CVE-2008-5161详细信息

问题

在您升级代码到7.0(3)I2(1)后，您无法对SSH到连结9000并且收到此错误：

```
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

原因您无法对SSH到连结9000，在您升级编码7.0(3)I2(1)后及以后弱密码器通过Cisco Bug ID CSCuv39937修正禁用。

此问题的长期解决方案将使用安排旧有弱密码器禁用的更新/最新的SSH客户端。

临时解决方案是弱密码器在连结9000返回的添加。有临时解决方案的两个可能的选项，取决于编码版本。

临时选项1. SSH密码器模式弱命令(与NXOS 7.0(3)I4(6)或以上的联机)

- 介绍通过Cisco Bug ID CSCvc71792 -请实现瘤允许弱密码器aes128-cbc,aes192-cbc,aes256-cbc。
- 添加这些弱密码器的支持- aes128-cbc、aes192-cbc和aes256-cbc。
- 仍有3DES CBC密码器的**没有支持**。

```
! baseline: only strong Ciphers aes128-ctr,aes192-ctr,aes256-ctr allowed
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。请使用贝斯为了修改sshd_config文件和明确地重新加写弱密码器

如果注释密码器线路从/isan/etc/sshd_config文件，支持所有默认密码器(这包括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
```

注意，当您补充说时旧有密码器返回您将使用弱密码器并且它是安全风险。