Cannot SSH into Nexus 9000 with "no matching cipher found" Error Received

Contents

Introduction

This document describes how to troubleshoot/resolve SSH issues to a Nexus 9000 after a code upgrade.

Background

Before the cause of the SSH issues are explained, it is necessary to know about the 'SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled' vulnerability which affects the Nexus 9000 platform.

CVE ID - CVE- 2008-5161 (SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled)

Issue description - SSH Server CBC Mode Ciphers Enabled Vulnerability (SSH Server CBC Mode Ciphers Enabled)

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This can allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Recommended solution - Disable CBC mode cipher encryption, and enable counter (CTR) mode or Galois/Counter Mode (GCM) cipher mode encryption

Reference - National Vulnerability Database - CVE-2008-5161 Detail

Problem

After you upgrade the code to 7.0(3)I2(1), you are unable to SSH into the Nexus 9000 and receive this error:

```
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
```

Solution

The reason you are unable to SSH into the Nexus 9000 after you upgrade to code 7.0(3)I2(1) and later is weak ciphers are disabled via the Cisco bug ID CSCuv39937 fix.

The long term solution for this problem is to use the updated/latest SSH client which has old weak ciphers disabled.

The temporary solution is to add weak ciphers back on the Nexus 9000. There are two possible options for the temporary solution, which depends on the version of code.

Temporary Option 1. ssh cipher-mode weak Command (Available with NXOS 7.0(3)I4(6) or Later)

- Introduced by Cisco bug ID CSCvc71792 - implement a knob to allow weak ciphers aes128-cbc,aes192-cbc,aes256-cbc.
- Adds support for these weak ciphers - aes128-cbc, aes192-cbc, and aes256-cbc.
- There is still **no support** for 3des-cbc cipher.

```
! 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
```

Temporary Option 2. Use Bash in Order to Modify the sshd_config File and Explicitly Re-add the Weak Ciphers

If you comment out the cipher line from the /isan/etc/sshd_config file, all default ciphers are supported (this includes aes128-cbc, **3des-cbc**, aes192-cbc, and 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
```

Note that when you add old ciphers back you revert to the use of weak ciphers and hence it is a security risk.