Kan niet overschakelen naar Nexus 9000 met "geen overeenkomend algoritme gevonden" fout ontvangen

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen met SSH kunt oplossen/oplossen in een Nexus 9000 na een upgrade van de code.

Achtergrond

Voordat de oorzaak van de SSH problemen wordt uitgelegd, is het noodzakelijk om te weten over de 'SSH Server CBC Mode CBC-coderingen Enabled & SSH Weak MAC Algorithms Enabled' kwetsbaarheid die van invloed is op het Nexus 9000 platform.

CVE-id - CVE-2008-5161 (SSH-server, CBC-modemcodering ingeschakeld en SSH zwakke MAC-algoritmen ingeschakeld)

Probleembeschrijving - SSH Server CBC Mode Crypters Enabled Vulnerability (SSH Server CBC Mode CCIPHERS Enabled)

De SSH-server is geconfigureerd om CBC-codering (Cpher Block Chaining) te ondersteunen. Dit kan een aanvaller toestaan om het plaintext bericht van de ciphertext terug te krijgen. Let op dat deze plug-in alleen controleert op de opties van de SSH server en niet controleert op kwetsbare softwareversies.

Aanbevolen oplossing - Schakel de codering van het algoritme voor de CBC-modus uit en schakel de CTR-modus of de codering van de Galois/Counter Mode (GCM) in

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

Probleem

Nadat u de code hebt geüpgraded naar 7.0(3)I2(1), kunt u niet overschakelen naar de Nexus 9000

en deze fout ontvangen:

```
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
```

Oplossing

De reden dat u niet in staat bent om SSH in de Nexus 9000 nadat u hebt geupgrade naar code 7.0(3)I2(1) en later is zwakke algoritmen zijn uitgeschakeld via de Cisco bug ID CSCuv39937 fix.

De oplossing op lange termijn voor dit probleem is om de bijgewerkte/nieuwste SSH-client te gebruiken die oude zwakke algoritmen uitgeschakeld heeft.

De tijdelijke oplossing is om zwakke algoritmen toe te voegen aan de Nexus 9000. Er zijn twee mogelijke opties voor de tijdelijke oplossing, die afhankelijk is van de versie van code.

Tijdelijke optie 1. ssh-algoritme-mode zwakke opdracht (beschikbaar met NXOS 7.0(3)I4(6) of hoger)

- Geïntroduceerd door Cisco bug-id CSCvc71792 - implementeer een knop om zwakke algoritmen aes128-cbc,aes192-cbc,aes256-cbc toe te staan.
- Voegt ondersteuning toe voor deze zwakke algoritmen - aes128-cbc, aes192-cbc en aes256-cbc.
- Er is nog steeds **geen ondersteuning** voor 3des-cbc algoritme.

```
! 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
```

Tijdelijke optie 2. Gebruik Bash om het sshd_config bestand te wijzigen en voeg

expliciet de zwakke coderingen toe

Als u de algoritme regel van het /isan/etc/sshd_config bestand becommentarieert, worden alle standaard algoritmen ondersteund (waaronder aes128-cbc, **3des-cbc**, aes192-cbc en 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
```

Merk op dat wanneer u oude algoritmen terug toevoegt u aan het gebruik van zwakke algoritmen terugkeert en vandaar het een veiligheidsrisico is.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.