Nexus 9000에 SSH를 연결할 수 없습니다. "일치하는 암호를 찾을 수 없음" 오류 수신

목차

소개

이 문서에서는 코드 업그레이드 후 Nexus 9000에 대한 SSH 문제를 트러블슈팅/해결하는 방법에 대해 설명합니다.

SSH 문제의 원인을 설명하기 전에 Nexus 9000 플랫폼에 영향을 주는 'SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled' 취약성에 대해 알아야 합니다.

CVE ID - CVE-2008-5161(SSH 서버 CBC 모드 암호 사용 및 SSH Weak MAC 알고리즘 사용)

문제 설명 - SSH 서버 CBC 모드 암호 사용 취약성(SSH 서버 CBC 모드 암호 사용)

SSH 서버는 CBC(Cipher Block Chaining) 암호화를 지원하도록 구성됩니다.이렇게 하면 공격자가 암호 텍스트에서 일반 텍스트 메시지를 복구할 수 있습니다.이 플러그인은 SSH 서버의 옵션만 확인하며 취약한 소프트웨어 버전을 확인하지 않습니다.

권장 솔루션 - CBC 모드 암호 암호화를 비활성화하고 CTR(Counter) 모드 또는 GCM(Galois/Counter Mode) 암호 모드 암호화를 활성화합니다.

참조 - 국가 취약성 데이터베이스 - CVE-2008-5161 세부사항

문제

코드를 7.0(3)I2(1)로 업그레이드한 후에는 Nexus 9000에 SSH를 연결할 수 없으며 다음 오류가 발생합니다.

```
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
```

솔루션

코드 7.0(3)I2(1) 이상으로 업그레이드한 후 Nexus 9000에 SSH를 연결할 수 없는 이유는 Cisco 버그 ID CSCuv39937 픽스를 통해 약한 암호가 비활성화되었기 때문입니다.

이 문제의 장기적인 해결책은 오래된 약한 암호를 사용하지 않도록 설정한 업데이트/최신 SSH 클라이언트를 사용하는 것입니다.

임시 솔루션은 Nexus 9000에 약한 암호를 다시 추가하는 것입니다.임시 솔루션에는 코드의 버전에 따라 두 가지 옵션이 있습니다.

임시 옵션 1. ssh cipher-mode weak 명령(NXOS 7.0(3)I4(6) 이상에서 사용 가능)

- Cisco 버그 ID CSCvc71792 - 약한 암호 aes128-cbc,aes192-cbc,aes256-cbc를 허용하는 노브를 구현합니다.
- aes128-cbc, aes192-cbc 및 aes256-cbc와 같은 취약한 암호를 지원합니다.
- 3des-cbc 암호를 여전히 **지원하지 않습니다**.

```
! 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
```

임시 옵션 2. sshd_config 파일을 수정하고 비고정 암호를 명시적으로 다시 추가하려면 Bash를 사용합니다.

/isan/etc/sshd_config 파일에서 암호 줄을 주석 처리하면 모든 기본 암호가 지원됩니다(aes128-cbc, **3des-cbc**, aes192-cbc 및 aes256-cbc 포함).

```
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
```

이전 암호를 다시 추가할 때 약한 암호를 사용하므로 보안 위험이 있습니다.