Impossibile eseguire SSH in Nexus 9000 con "nessuna cifratura corrispondente trovata" Errore ricevuto

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi SSH su un Nexus 9000 dopo un aggiornamento del codice.

Sfondo

Prima di spiegare la causa dei problemi SSH, è necessario conoscere la vulnerabilità 'SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled' che influisce sulla piattaforma Nexus 9000.

ID CVE - CVE- 2008-5161 (crittografia modalità CBC server SSH abilitata e algoritmi MAC vulnerabili SSH abilitati)

Descrizione del problema - Vulnerabilità abilitata per la crittografia in modalità CBC del server SSH (abilitata per la crittografia in modalità CBC del server SSH)

Il server SSH è configurato per supportare la crittografia CBC (Cipher Block Chaining). In questo modo l'autore di un attacco può recuperare il messaggio non crittografato dal testo cifrato. Notare che questo plug-in controlla solo le opzioni del server SSH e non le versioni software vulnerabili.

Soluzione consigliata: disabilitare la crittografia cifratura in modalità CBC e abilitare la modalità contatore (CTR) o la crittografia in modalità cifratura Galois/Counter (GCM)

Riferimento - [Database nazionale sulle vulnerabilità - CVE-2008-5161 Dettaglio](#)

Problema

Dopo aver aggiornato il codice alla versione 7.0(3)I2(1), non è possibile eseguire il protocollo SSH su Nexus 9000 e viene visualizzato questo messaggio di errore:

```
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
```

Soluzione

La ragione per cui non è possibile eseguire il protocollo SSH su Nexus 9000 dopo aver eseguito l'aggiornamento al codice 7.0(3)I2(1) e versioni successive è che le cifrature deboli sono state disabilitate con la correzione del bug Cisco con ID CSCuv39937.

La soluzione a lungo termine per questo problema è usare il client SSH aggiornato/più recente con le vecchie cifrature deboli disabilitate.

La soluzione temporanea consiste nell'aggiungere di nuovo delle cifrature deboli sul Nexus 9000. Sono disponibili due opzioni per la soluzione temporanea, che dipende dalla versione del codice.

Opzione temporanea 1. Comando ssh cipher-mode weak (disponibile con NXOS 7.0(3)I4(6) o versioni successive)

- Introdotta da Cisco, l'ID bug CSCvc71792: implementa una manopola per consentire le cifrature deboli aes128-cbc,aes192-cbc,aes256-cbc.
- Aggiunge il supporto per queste cifrature deboli - aes128-cbc, aes192-cbc e aes256-cbc.
- La cifratura 3des-cbc **non è** ancora **supportata**.

```
! 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
```

Opzione temporanea 2. Utilizzare Bash per modificare il file sshd_config e riaggiungere esplicitamente i cifrari deboli

Se si commenta la riga di cifratura dal file /isan/etc/sshd_config, sono supportate tutte le cifrature predefinite (incluse aes128-cbc, **3des-cbc**, aes192-cbc e 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
```

Si noti che quando si ripristinano vecchie cifrature, si torna all'uso di cifrature deboli e ciò costituisce un rischio per la sicurezza.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).