Keine SSH-Verbindung zum Nexus 9000 mit "kein übereinstimmender Schlüssel gefunden" Fehler empfangen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie SSH-Probleme beim Nexus 9000 nach einem Code-Upgrade behoben werden.

Hintergrund

Bevor die Ursache der SSH-Probleme erklärt wird, muss die Schwachstelle 'SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled' bekannt sein, die die Nexus 9000-Plattform betrifft.

CVE-ID - CVE-2008-5161 (SSH-Server CBC-Modus-Verschlüsselungen aktiviert und SSH Weak MAC Algorithms aktiviert)

Problembeschreibung - Sicherheitslücke bei CBC-Modus-Ciphers des SSH-Servers aktiviert (CBC-Modus-Ciphers des SSH-Servers aktiviert)

Der SSH-Server ist so konfiguriert, dass er die Verschlüsselung durch CBC (Cipher Block Chaining) unterstützt. Dadurch kann ein Angreifer die Klartextnachricht aus dem Chiffretext wiederherstellen. Beachten Sie, dass dieses Plug-in nur die Optionen des SSH-Servers überprüft und nicht nach anfälligen Softwareversionen.

Empfohlene Lösung - Verschlüsselung im CBC-Modus deaktivieren und Verschlüsselung im CTR-Modus oder Galois-/GCM-Verschlüsselungsmodus aktivieren

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

Problem

Nachdem Sie den Code auf 7.0(3)I2(1) aktualisiert haben, können Sie keine SSH-Verbindung zum

Nexus 9000 herstellen und erhalten den folgenden Fehler:

```
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
```

Lösung

Der Grund, warum Sie nach dem Upgrade auf Code 7.0(3)I2(1) nicht in der Lage sind, SSH auf den Nexus 9000 zu installieren, und später ist, dass schwache Chiffren über die Cisco Bug-ID CSCuv39937 behoben werden.

Die langfristige Lösung für dieses Problem besteht darin, den aktualisierten/neuesten SSH-Client zu verwenden, der alte schwache Chiffren deaktiviert hat.

Die temporäre Lösung besteht darin, dem Nexus 9000 schwache Chiffren hinzuzufügen. Für die temporäre Lösung, die von der Codeversion abhängt, gibt es zwei mögliche Optionen.

Temporäre Option 1. ssh cipher-mode weaked Command (verfügbar mit NXOS 7.0(3)I4(6) oder höher)

- Einführung durch Cisco Bug-ID CSCvc71792 - Implementieren Sie einen Knopf, um schwache Chiffren zu ermöglichen: aes128-cbc,aes192-cbc,aes256-cbc.
- Fügt Unterstützung für diese schwachen Chiffren hinzu - aes128-cbc, aes192-cbc und aes256-cbc.
- Es gibt immer noch **keine Unterstützung** für die 3des-cbc-Verschlüsselung.

```
! 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
```

Vorübergehende Option 2. Verwenden Sie Bash, um die Datei sshd_config zu ändern und die schwachen Chiffren explizit erneut hinzuzufügen.

Wenn Sie die Chiffrierzeile aus der Datei /isan/etc/sshd_config kommentieren, werden alle Standardchiffren unterstützt (dazu gehören aes128-cbc, **3des-cbc,** aes192-cbc und 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
```

Beachten Sie, dass wenn Sie alte Chiffren wieder hinzufügen, Sie auf die Verwendung von schwachen Chiffren und daher ist es ein Sicherheitsrisiko.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.