Impossible d'établir une connexion SSH dans Nexus 9000 avec " ; aucun chiffre correspondant trouvé" ; Erreur reçue

Table des matières

Introduction

Ce document décrit comment dépanner/résoudre des problèmes SSH sur un Nexus 9000 après une mise à niveau de code.

Fond

Avant d'expliquer la cause des problèmes SSH, il est nécessaire de connaître la vulnérabilité « SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled » qui affecte la plate-forme Nexus 9000.

CVE ID - CVE- 2008-5161 (Serveur SSH - Chiffrement en mode CBC activé et Algorithmes MAC faibles SSH activés)

Description du problème - Vulnérabilité activée pour le chiffrement en mode CBC du serveur SSH (Activation pour le chiffrement en mode CBC du serveur SSH)

Le serveur SSH est configuré pour prendre en charge le chiffrement CBC (Cipher Block Chaining). Cela peut permettre à un attaquant de récupérer le message en texte clair à partir du texte chiffré. Notez que ce plug-in vérifie uniquement les options du serveur SSH et ne vérifie pas les versions logicielles vulnérables.

Solution recommandée : désactivez le chiffrement en mode CBC et activez le chiffrement en mode compteur (CTR) ou Galois/Counter Mode (GCM)

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

Problème

Après avoir mis à niveau le code vers 7.0(3)I2(1), vous ne pouvez pas SSH dans le Nexus 9000 et

recevoir cette erreur :

```
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

La raison pour laquelle vous ne pouvez pas SSH dans le Nexus 9000 après la mise à niveau vers le code 7.0(3)I2(1) et plus tard est que les chiffrements faibles sont désactivés via l'ID de bogue Cisco CSCuv3937 correctif.

La solution à long terme pour ce problème est d'utiliser le client SSH mis à jour/le plus récent dont les anciens chiffrements faibles sont désactivés.

La solution temporaire consiste à ajouter des chiffrements faibles sur le Nexus 9000. Il y a deux options possibles pour la solution temporaire, qui dépend de la version du code.

Option temporaire 1. Commande ssh cipher-mode faible (disponible avec NXOS 7.0(3)I4(6) ou version ultérieure)

- Introduit par le bogue Cisco ID CSCvc71792 - mettre en oeuvre un bouton pour permettre des chiffrements faibles aes128-cbc, aes192-cbc, aes256-cbc.
- Ajoute la prise en charge de ces chiffrements faibles : aes128-cbc, aes192-cbc et aes256-cbc.
- Le chiffrement 3des-cbc **n'**est toujours **pas pris en charge**.

```
! 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
```

Option temporaire 2. Utilisez Bash afin de modifier le fichier sshd_config et de rajouter explicitement les chiffrements faibles

Si vous commentez la ligne de chiffrement à partir du fichier /isan/etc/sshd_config, tous les chiffrements par défaut sont pris en charge (cela inclut aes128-cbc, **3des-cbc**, aes192-cbc et 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
```

Notez que lorsque vous rajoutez d'anciens chiffrements, vous retournez à l'utilisation de chiffrements faibles, ce qui représente un risque pour la sécurité.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.