Incapable au SSH dans le Nexus 9000 avec « aucun chiffrement assorti fondez » l'erreur reçue

Contenu

Introduction

Ce document décrit comment dépanner/des questions SSH de résolution à un Nexus 9000 après une mise à niveau du code.

Avant la cause des questions de SSH sont expliqués, il est nécessaire de savoir « le mode CBC de serveur de SSH chiffre la vulnérabilité activée par algorithmes faibles activée et de SSH de MAC » qui affecte la plate-forme du Nexus 9000.

ID CVE - CVE 2008-5161 (le mode CBC de serveur de SSH chiffre les algorithmes faibles activée et de SSH de MAC activés)

Description de question - Les chiffrements de mode CBC de serveur de SSH ont activé la vulnérabilité (les chiffrements de mode CBC de serveur de SSH activés)

Le serveur de SSH est configuré pour prendre en charge le bloc de chiffrement enchaînant le cryptage (CBC). Ceci pourrait permettre à un attaquant pour récupérer le message de plaintext du cryptogramme. Notez que ce module d'extension vérifie seulement les options du serveur de SSH et ne vérifie pas les versions de logiciel vulnérables.

Solution recommandée - Cryptage de chiffrement de mode CBC de débronchement, et mode d'enable contre- (CTR) ou Galois/cryptage de mode de chiffrement mode de compteur (GCM)

Référence - Base de données nationale de vulnérabilité - Détail CVE-2008-5161

Problème

Après que vous amélioriez le code à 7.0(3)I2(1), vous ne pouvez pas au SSH dans le Nexus 9000 et recevez 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 vous ne pouvez pas au SSH dans le Nexus 9000 après que vous amélioriez pour coder 7.0(3)I2(1) et plus tard est les chiffrements faibles sont désactivés par l'intermédiaire de la difficulté de l'ID de bogue Cisco CSCuv39937.

La solution à long terme pour ce problème est d'utiliser le mis à jour/le plus tard le client SSH qui fait désactiver de vieux chiffrements faibles.

La solution provisoire est d'ajouter des chiffrements faibles arrières sur le Nexus 9000. Il y a deux choix possibles pour la solution provisoire, qui dépend de la version du code.

Commande faible de l'option 1. de chiffrement-mode provisoire de ssh (disponible avec NXOS 7.0(3)I4(6) ou plus tard)

- Introduit par l'intermédiaire de l'ID de bogue Cisco CSCvc71792 - implémentez une molette pour permettre les chiffrements faibles aes128-cbc,aes192-cbc,aes256-cbc.
- Ajoute le soutien de ces chiffrements faibles - aes128-cbc, aes192-cbc, et aes256-cbc.
- Il ne reste **aucun soutien du** chiffrement 3des-cbc.

```
! 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
```

Option 2 provisoire. Employez le coup afin de modifier le fichier de sshd_config et Re-ajouter explicitement les chiffrements faibles

Si vous commentez la ligne de chiffrement à partir du fichier de /isan/etc/sshd_config, tous les chiffrements par défaut sont pris en charge (ceci 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 quand vous ajoutez de vieux chiffrements vous soutiennent utilisera des chiffrements faibles et par conséquent c'est un risque de sécurité.