No se puede SSH en Nexus 9000 con "no se ha encontrado ningún cifrado que coincida" Error recibido

Contenido

Introducción

Este documento describe cómo resolver problemas de SSH en un Nexus 9000 después de una actualización de código.

Background

Antes de explicar la causa de los problemas de SSH, es necesario conocer la vulnerabilidad 'SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled' que afecta a la plataforma Nexus 9000.

CVE ID - CVE- 2008-5161 (cifrado de modo CBC de servidor SSH habilitado y algoritmos MAC débiles de SSH habilitados)

Descripción del problema - Vulnerabilidad activada por los cifradores de modo CBC del servidor SSH (activación de los cifradores de modo CBC del servidor SSH)

El servidor SSH está configurado para soportar el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado. Tenga en cuenta que este plugin solo verifica las opciones del servidor SSH y no verifica las versiones de software vulnerables.

Solución recomendada: desactive el cifrado en modo CBC y active el cifrado en modo contador (CTR) o en modo Galois/Counter (GCM)

Referencia - [Base de datos nacional de vulnerabilidades - CVE-2008-5161 Detalle](#)

Problema

Después de actualizar el código a 7.0(3)I2(1), no puede introducir SSH en el Nexus 9000 y recibir

este error:

```
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
```

Solución

La razón por la que no puede realizar SSH en el Nexus 9000 después de actualizar al código 7.0(3)I2(1) y posteriores es que los cifrados débiles están desactivados a través del ID de bug Cisco CSCuv39937.

La solución a largo plazo para este problema es utilizar el cliente SSH actualizado/más reciente que tiene los cifrados débiles viejos inhabilitados.

La solución temporal consiste en volver a agregar cifrados débiles al Nexus 9000. Hay dos opciones posibles para la solución temporal, que depende de la versión del código.

Opción temporal 1. Comando ssh cipher-mode weak (disponible con NXOS 7.0(3)I4(6) o posterior)

- Introducido por el ID de bug de Cisco CSCvc71792 - implemente un botón para permitir los cifrados débiles aes128-cbc,aes192-cbc,aes256-cbc.
- Añade compatibilidad con estos cifrados débiles: aes128-cbc, aes192-cbc y aes256-cbc.
- Todavía **no** hay **soporte** para 3des-cbc cipher.

```
! 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
```

Opción temporal 2. Utilice Bash para modificar el archivo sshd_config y volver a

agregar explícitamente los cifrados débiles

Si comenta la línea de cifrado desde el archivo /isan/etc/sshd_config, se soportan todos los cifrados predeterminados (esto incluye aes128-cbc, **3des-cbc**, aes192-cbc y 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
```

Tenga en cuenta que cuando vuelva a agregar cifrados antiguos, volverá al uso de cifrados débiles y, por tanto, supondrá un riesgo para la seguridad.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).