Incapaz a SSH en el nexo 9000 con “ningún” error encontrado cifra que corresponde con recibido

Contenido

Introducción

Este documento describe cómo resolver problemas/los problemas de SSH de la resolución a un nexo 9000 después de una actualización de código.

Antes de la causa de los problemas de SSH se explican, es necesario saber sobre el “servidor SSH que el modo CBC cifra la vulnerabilidad habilitada los algoritmos débiles habilitada y de SSH MAC” que afecta a la plataforma del nexo 9000.

CVE ID - CVE 2008-5161 (el modo CBC del servidor SSH cifra los algoritmos débiles habilitados y de SSH MAC habilitados)

Descripción del problema - Vulnerabilidad habilitada de las cifras del modo CBC del servidor SSH (cifras del modo CBC del servidor SSH habilitadas)

Configuran al servidor SSH para soportar el cifrado del Cipher Block Chaining (CBC). Esto pudo permitir que un atacante recupere el mensaje del texto simple del texto cifrado. Observe que este solamente las comprobaciones para plugs-in las opciones del servidor SSH y no marca para saber si hay versiones de software vulnerables.

Solución recomendada - Inhabilite el cifrado de la cifra del modo CBC, y habilite al revés (CTR) el modo o Galois/el cifrado contrario del modo de la cifra del modo (GCM)

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

Problema

Después de que usted actualice el código a 7.0(3)I2(1), usted no puede a SSH en el nexo 9000 y recibe 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 usted no puede a SSH en el nexo 9000 después de que usted actualice para cifrar 7.0(3)I2(1) y posterior sea cifras débiles se inhabilite vía el arreglo del Id. de bug Cisco CSCuv39937.

La solución a largo plazo para este problema es utilizar al cliente SSH actualizado/último que hace las viejas cifras débiles inhabilitar.

La solución temporaria es agregar las cifras débiles posteriores en el nexo 9000. Hay dos opciones posibles para la solución temporaria, que depende de la versión del código.

Comando débil temporal del ssh cifra-MODE de la opción 1. (disponible con NXOS 7.0(3)I4(6) o más adelante)

- Introducido vía el Id. de bug Cisco CSCvc71792 - implemente un botón para permitir las cifras débiles aes128-cbc,aes192-cbc,aes256-cbc.
- Agrega el soporte para estas cifras débiles - aes128-cbc, aes192-cbc, y aes256-cbc.
- Todavía no hay **soporte** para la cifra 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
```

Opción temporal 2. Utilice el golpe para modificar el archivo del sshd_config y Re-agregar explícitamente las cifras débiles

Si usted comenta hacia fuera la línea de la cifra del archivo de /isan/etc/sshd_config, se soportan todas las cifras del valor por defecto (ésta 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
```

Observe que cuando usted agrega las viejas cifras le apoyan utilizará las cifras débiles y por lo tanto es un riesgo de seguridad.