Incapaz ao SSH no nexo 9000 com “nenhum” erro encontrado cifra de harmonização recebido

Índice

Introdução

Este documento descreve como pesquisar defeitos/edições da resolução SSH a um nexo 9000 após uma upgrade de código.

Antes da causa das edições SSH são explicados, é necessário saber sobre do “o modo de CBC servidor de SSH calcula a vulnerabilidade permitida permitida & SSH MAC algoritmos fracos” que afeta a plataforma do nexo 9000.

CVE ID - CVE 2008-5161 (o modo de CBC do servidor de SSH calcula os algoritmos fracos permitida & SSH MAC permitidos)

Descrição da edição - As cifras do modo de CBC do servidor de SSH permitiram a vulnerabilidade (as cifras do modo de CBC do servidor de SSH permitidas)

O servidor de SSH é configurado para apoiar a criptografia do Cipher Block Chaining (CBC). Isto pôde permitir que um atacante recupere a mensagem do texto simples do texto cifrado. Note que este somente verificações de encaixe para as opções do servidor de SSH e não o verifique para ver se há versões de software vulneráveis.

Solução recomendada - Desabilite a criptografia da cifra do modo de CBC, e permita contra o modo (CTR) ou o Galois/criptografia contrária do modo da cifra do modo (GCM)

Referência - [Base de dados nacional da vulnerabilidade - Detalhe CVE-2008-5161](#)

Problema

Depois que você promove o código a 7.0(3)I2(1), você é incapaz ao SSH no nexo 9000 e recebe este erro:

```
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
```

Solução

A razão você é incapaz ao SSH no nexo 9000 depois que você promove para codificar 7.0(3)I2(1) e mais atrasadas estão as cifras fracas estão desabilitadas através do reparo da identificação de bug Cisco CSCuv39937.

A solução a longo prazo para este problema é usar o actualizado/o mais tarde o cliente SSH que tem cifras fracas velhas desabilitadas.

A solução temporária é adicionar as cifras fracas traseiras no nexo 9000. Há duas opções possíveis para a solução temporária, que depende da versão de código.

Comando fraco provisório do ssh cifra-MODE da opção 1. (disponível com NXOS 7.0(3)I4(6) ou mais atrasado)

- Introduzido através da identificação de bug Cisco CSCvc71792 - execute um botão para permitir as cifras fracas aes128-cbc,aes192-cbc,aes256-cbc.
- Adiciona o apoio para estas cifras fracas - aes128-cbc, aes192-cbc, e aes256-cbc.
- Não há ainda **nenhum apoio** para a 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
```

Opção provisória 2. Use a festança a fim alterar o arquivo do sshd_config e adicionar novamente explicitamente as cifras fracas

Se você comenta para fora a linha da cifra do arquivo de /isan/etc/sshd_config, todas as cifras do padrão estão apoiadas (esta inclui aes128-cbc, **3des-cbc**, aes192-cbc, e 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
```

Note que quando você adiciona cifras velhas o suportam usará cifras fracas e daqui é um risco de segurança.