Não é possível executar SSH no Nexus 9000 com "nenhuma codificação correspondente encontrada" Erro recebido

Contents

Introduction

Este documento descreve como solucionar/resolver problemas de SSH para um Nexus 9000 após uma atualização de código.

Background

Antes que a causa dos problemas de SSH sejam explicados, é necessário saber sobre a vulnerabilidade 'SSH Server CBC Mode Ciphers Enabled & SSH Weak MAC Algorithms Enabled' que afeta a plataforma Nexus 9000.

ID do CVE - CVE- 2008-5161 (Cifras do modo CBC do servidor SSH ativadas e algoritmos MAC fracos do SSH ativados)

Descrição do problema - Vulnerabilidade de cifras no modo CBC do servidor SSH habilitada (Cifras no modo CBC do servidor SSH habilitadas)

O servidor SSH está configurado para suportar a criptografia CBC (Cipher Block Chaining). Isso pode permitir que um invasor recupere a mensagem de texto simples do texto cifrado. Note que este plugin só verifica as opções do servidor SSH e não verifica as versões de software vulneráveis.

Solução recomendada - Desabilite a criptografia de cifra no modo CBC e habilite o modo de contador (CTR) ou a criptografia no modo Galois/Counter Mode (GCM)

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

Problema

Depois de atualizar o código para 7.0(3)I2(1), você não consegue fazer SSH no Nexus 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 pela qual você não consegue fazer SSH no Nexus 9000 após a atualização para o código 7.0(3)I2(1) e posterior é que cifras fracas são desativadas através da correção do ID de bug Cisco CSCuv3937.

A solução de longo prazo para este problema é usar o cliente SSH atualizado/mais recente que tem cifras fracas antigas desabilitadas.

A solução temporária é adicionar cifras fracas de volta no Nexus 9000. Há duas opções possíveis para a solução temporária, que depende da versão do código.

Opção temporária 1. Comando ssh cipher-mode weak (disponível com NXOS 7.0(3)I4(6) ou posterior)

- Introduzido pelo bug da Cisco ID CSCvc71792 - implemente um botão para permitir cifras fracas aes128-cbc,aes192-cbc,aes256-cbc.
- Adiciona suporte para essas cifras fracas - aes128-cbc, aes192-cbc e aes256-cbc.
- Ainda não há **suporte** para cifra 3des-cbc.

```
! 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
```

Opção Temporária 2. Use Bash para modificar o arquivo sshd_config e readicionar

explicitamente as cifras fracas

Se você comentar a linha de cifra do arquivo /isan/etc/sshd_config, todas as cifras padrão serão suportadas (isso 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
```

Observe que quando você adiciona cifras antigas de volta, você reverte para o uso de cifras fracas e, portanto, é um risco de segurança.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.