受け取った「一致する暗号によって検出される」エラー無しの Nexus 9000 に SSH にない

目次

概要

この資料にコードアップグレードの後で Nexus 9000 に/解決 SSH 問題解決する方法を記述されています。

SSH の原因の前に問題は説明されます、「SSH サーバ CBC モードについて確認することは必要暗号化します Nexus 9000 プラットフォームに影響を与えるイネーブルになった及び SSH 弱い MAC アルゴリズムによってイネーブルになられている」脆弱性をです。

CVE ID - CVE- 2008-5161（SSH サーバ CBC はモードはイネーブルになっているイネーブルになった及び SSH 弱い MAC アルゴリズムを暗号化します）

問題説明- SSH サーバ CBC モードはイネーブルになった脆弱性（イネーブルになっている SSH サーバ CBC モード暗号）を暗号化します

SSH サーバは Cipher Block Chaining（CBC）暗号化をサポートするために設定されます。 これは攻撃者が暗号文からプレーンテキスト メッセージを回復ことを可能にするかもしれません。 このプラグインが SSH サーバのオプションがあるようにのためにだけ確認し、脆弱なソフトウェア バージョンがあるように確認しないことに注目して下さい。

推奨される ソリューション- CBC モード暗号暗号化および Enable カウンター（CTR）モードまたは Galois/カウンター モード（GCM）暗号モード暗号化ディセーブルにして下さい

参照- National 脆弱性データベース- CVE-2008-5161 詳細

問題

7.0(3)I2(1) にコードをアップグレードした後、Nexus 9000 に SSH になく、このエラーを受け取ります:

```
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
```

解決策

7.0(3)I2(1) およびそれ以降をコードするためにである弱い暗号である Cisco バグ ID CSCuv39937 修正によって無効アップグレードした後原因 Nexus 9000 に SSH にないです。

この問題のための長期ソリューションはディセーブルにされる古く弱い暗号がある更新済を/最も遅く SSH クライアントを使用することです。

一時ソリューションは Nexus 9000 で背部弱い暗号を追加することです。 一時ソリューションのための 2 つの可能性のあるオプションがあります、コードのバージョンによって決まる。

一時オプション 1. ssh 暗号モード弱いコマンド (NXOS 7.0(3)I4(6) またはそれ以降と利用可能な)

- Cisco バグ ID CSCvc71792 によって導入されて-弱い暗号 aes128-cbc,aes192-cbc,aes256-cbc を許可するためにノブを設定して下さい。
- これらの弱い暗号のサポートを- aes128-cbc、aes192-cbc および aes256-cbc 追加します。
- 今でもトリプル DES CBC 暗号の**サポートが**ありません。

```
! 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
```

一時オプション 2。 sshd_config ファイルを修正し、明示的に弱い暗号を再追加するために Bash を使用して下さい

暗号行 /isan/etc/sshd_config ファイルからのコメントになる場合、すべてのデフォルト暗号はサポートされます (これには aes128-cbc、トリプル DES **CBC**、aes192-cbc および aes256-cbc が含まれています) 。

```
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
```

付け加えるときことに古い暗号支持する使用する弱い暗号を注目すればそれ故にそれはセキュリティリスクです。