# "；でNexus 9000にSSHできません。一致する暗号が見つかりません"；エラーを受信しました

## 内容



## 概要

このドキュメントでは、コードのアップグレード後にNexus 9000に対するSSHの問題をトラブルシューティングおよび解決する方法について説明します。

## 背景

SSHの問題の原因を説明する前に、Nexus 9000プラットフォームに影響を与える「SSHサーバCBCモード暗号が有効でSSH弱いMACアルゴリズムが有効」の脆弱性について知っておく必要があります。

CVE ID:CVE-2008-5161（SSHサーバのCBCモードの暗号が有効で、SSHの脆弱なMACアルゴリズムが有効）

問題の説明：SSHサーバのCBCモードで暗号機能が有効になっている脆弱性（SSHサーバのCBCモードで暗号機能が有効になっている）

SSHサーバは、Cipher Block Chaining(CBC)暗号化をサポートするように設定されています。これにより、攻撃者は暗号文からプレーンテキストメッセージを回復できる可能性があります。このプラグインはSSHサーバのオプションのみをチェックし、脆弱なソフトウェアバージョンはチェックしないことに注意してください。

推奨ソリューション：CBCモードの暗号化を無効にし、カウンタ(CTR)モードまたはGalois/Counter Mode(GCM)暗号化モードの暗号化を有効にします

参考：National Vulnerability Database - CVE-2008-5161詳細

## 問題

コードを7.0(3)I2(1)にアップグレードした後、Nexus 9000にSSH接続できず、次のエラーが表示されます。

```
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
```

# 解決方法

コード7.0(3)I2(1)以降にアップグレードした後、Nexus 9000にSSH接続できない理由は、脆弱な暗号がCisco Bug ID CSCuv39937の修正によって無効になっているためです。

この問題の長期的な解決策は、古い脆弱な暗号が無効になっている最新のSSHクライアントを使用することです。

一時的な解決策は、Nexus 9000に弱い暗号を追加し直すことです。コードのバージョンに応じて、一時的な解決策には2つのオプションがあります。

## 一時的なオプション1:ssh cipher-mode weakコマンド(NXOS 7.0(3)I4(6)以降で使用可能)

- Cisco Bug ID CSCvc71792で導入された：弱い暗号aes128-cbc、aes192-cbc、aes256-cbcを許可するノブを実装します。
- これらの弱い暗号aes128-cbc、aes192-cbc、およびaes256-cbcのサポートを追加します。
- 3des-cbc暗号はまだサポートされていません。

```
! 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
```

## 一時オプション2:sshd_configファイルを変更し、脆弱な暗号を明示的に再追加するためにBashを使用する

/isan/etc/sshd_configファイルから暗号行をコメントアウトすると、すべてのデフォルトの暗号が

サポートされます(aes128-cbc、3des-cbc、aes192-cbc、およびaes256-cbcを含みます)。

```
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
```

古い暗号を追加すると、弱い暗号の使用に戻るため、セキュリティ上のリスクがあることに注意してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。