# NCCM 3.8+およびCSPC 2.9+のCBC暗号の脆弱性のトラブルシューティング

## 内容



## はじめに

このドキュメントでは、NCCM 3.8+およびCSPC 2.9+のCBC暗号の脆弱性をトラブルシューティングする方法について説明します。

## 問題

CSPC/NCCMの最近のリリースでは、CBCの脆弱な暗号の脆弱性が存在します。ほとんどの場合、目的のssh設定ファイルを更新することで修正できます。ただし、この記事は、暗号ポリシーを使用して明示的にアクセスを拒否するように挙げられています。他のすべてが失敗した場合はこれを使用してください。これはデフォルトの暗号化ポリシーには影響せず、デフォルトポリシーの上に追加のレイヤを追加します。

### 従来のアプローチ

すべてのCVC暗号がsshd_configから削除されていることを確認します。問題がまだ解決しない場合は、/etc/sysconfig/sshdの下のパラメータに空白のエントリを指定できます。

```
CRYPTO_POLICY=
```

変更を行う前に、必ずバックアップを取ってください。

正しく動作していることを確認するには、リモートマシンで次のコマンドを実行します。

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

パスワードの入力やRSAキーの追加を求めるメッセージが表示されても、問題は解決しません。

# ソリューション

上記の手順が失敗した場合は、CBC暗号へのアクセスを明示的に拒否することで、暗号ポリシーのレイヤを追加できます。暗号ポリシーのデフォルト設定を変更することは推奨されません。そのため、この方法をお勧めします。

先に進む前に、DEFAULT暗号化ポリシーの上に追加のレイヤが適用されていないことを確認します。追加のレイヤがある場合は、変更を加える前にレイヤを確認できます。これを確認するには、次のコマンドを実行します。

```
update-crypto-policies --show
```

この応答はDEFAULTです。存在する場合は、それ以上の検証を行わずに次の手順に進むことができます。

絶対パスの下に新しいファイルを作成します。

```
/etc/crypto-policies/policies/modules/DISABLE-CBC.pmod
```

このファイルにはどのような名前を付けることもできますが、拡張子は.pmodで終わります。

これらの暗号を使用してsshアクセスを制限するために、この脆弱性を削除するため、この新しいファイルでは次の行のみをエントリとして入力します。

```
ssh_cipher = -AES-128-CBC -AES-256-CBC
```

---

注：これは参照用です。明示的に拒否しようとしているすべての暗号を追加できますが、混乱を避けるために、CBC以外のすべての暗号に対して新しいファイルを作成することをお勧めします。

---

ファイルを保存した後、次のコマンドを実行して、crypto-policiesの値をDEFAULTから、この追加レイヤに設定します。

```
update-crypto-policies --set DEFAULT:DISABLE-CBC
```

ここでも、DISABLE-CBCの値は、ファイルの作成時に指定した名前に基づいて異なる場合があります。

次のコマンドを実行して再確認できます。

```
update-crypto-policies --show
```

今回はDEFAULT:DISABLE-CBCと表示され、デフォルトファイルを変更せずにレイヤを追加したことが確認できます。

この段階で、アクセスを再検証すると、アクセスは拒否されます。

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

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。