ASA での SSH サーバ CBC モード暗号の無効化

内容

概要

このドキュメントでは、ASA で SSH サーバ CBC モードの暗号を無効にする方法について説明します。スキャンの脆弱性 CVE-2008-5161 には、暗号ブロック連鎖（CBC）モードでブロック暗号アルゴリズムを使用すると、リモート攻撃者が不明な経路を介して、SSH 内の任意の暗号テキストブロックから特定のプレーンテキストデータを簡単に回復できることが文書化されています。

暗号ブロック連鎖（CBC）は暗号ブロックの動作モードであり、このアルゴリズムはブロック暗号を使用して機密性や真正性などの情報サービスを提供します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 適応型セキュリティアプライアンス ASA プラットフォーム アーキテクチャ
- 暗号ブロック連鎖（CBC）

使用するコンポーネント

このドキュメントの情報は、OS 9.6.1 が稼働する Cisco ASA 5506 に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

デフォルトでは、ASA では CBC モードが有効になっているため、これは顧客情報にとって脆弱性となり得ます。

解決方法

CSCum63371 の改善後、ASA の SSH 暗号を変更する機能がバージョン 9.1(7) で導入されましたが、**ssh cipher encryption** コマンドと **ssh cipher integrity** コマンドが正式に含まれているリリースは 9.6.1 です。

SSH で CBC モード暗号を無効にするには、次の手順に従います。

ASA で「sh run all ssh」を実行します。

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption medium
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

ssh cipher encryption media コマンドが表示される場合、ASA ではデフォルトで設定されている中および高強度の暗号が使用されます。

ASA で使用可能な SSH 暗号化アルゴリズムを確認するには、**show ssh ciphers** コマンドを実行します。

```
ASA(config)# show ssh ciphers
Available SSH Encryption and Integrity Algorithms Encryption Algorithms:
       all:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       fips:    aes128-cbc   aes256-cbc
       high:    aes256-cbc   aes256-ctr
Integrity Algorithms:
       all:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
       low:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
       medium:  hmac-sha1    hmac-sha1-96
       fips:    hmac-sha1
       high:    hmac-sha1
```

出力には、次に示す使用可能なすべての暗号化アルゴリズムが表示されます。 **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。**

CBC モードを無効にして SSH 設定で使用できるようにするには、次のコマンドによって、使用する暗号化アルゴリズムをカスタマイズします。

```
ssh cipher encryption custom aes128-ctr:aes192-ctr:aes256-ctr
```

これが完了したら、コマンド **show run all ssh** を実行します。SSH 暗号化の設定では、すべてのアルゴリズムが CTR モードのみを使用するようになっています。

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
```

```
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption custom "aes128-ctr:aes192-ctr:aes256-ctr"
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

同様に、SSH 整合性アルゴリズムは、**ssh cipher integrity** コマンドを使用して変更できます。