目次

概要

シスコ コンフィギュレーション ファイル内のユーザ パスワード (およびその他のパスワード) を復号化するためのプログラムが、シスコ以外の情報源から公開されています。 このプログラムでは、enable secret コマンドで設定されたパスワードは復号化できません。 このプログラムを原因とする予想外の懸念がシスコのお客様の間に広がっていることから、シスコのパスワード暗号化を利用している方の多くが、仕様以上のセキュリティを期待しているのではないかと考えました。 この文書では、シスコのパスワード暗号化の背後にあるセキュリティ モデルと、この暗号化におけるセキュリティの限界について説明しています。

注シスコでは、すべての Cisco IOS デバイスで Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウンティング) セキュリティ モデルを実装することを推奨しています。 AAA ではローカル、RADIUS、および TACACS+ の各データベースを使用できます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ユーザ パスワード

Cisco IOS コンフィギュレーション ファイル内にあるユーザ パスワードと他の大部分のパスワード（enable secret ではありません）は、最新の暗号化規格に比べて非常に脆弱な方式を使用し暗号化されています。

Cisco が復号化 プログラムを配らないが、Cisco IOS パスワードのための少なくとも 2 つの異なる復号化プログラムはインターネットのパブリックに利用できます; Cisco がに気づいているそのようなプログラムの最初の一般公開は早い 1995 年にありました。 暗号に詳しい者であればだれでも簡単に新しいプログラムを作成できると考えられます。

Cisco IOS で使用しているユーザ パスワードの方式は、周到かつ巧妙な攻撃から守ることを意図して作られていませんでした。 この暗号化方式は、簡単なスヌーピングやスニフィングによるパスワードの漏洩を防ぐために開発されたものです。 コンフィギュレーション ファイルに対してパスワード クラッキングを試みる者からパスワードを保護するようには意図されていません。

暗号化アルゴリズムが脆弱であるため、シスコではコンフィギュレーション ファイルを機密情報として、クリアテキストのパスワード リストと同様に取り扱っていただくことを常にお客様にお願いしています。

enable secret と enable password

enable password コマンドは、今後は使用しないでください。 よりセキュリティに優れた **enable secret** コマンドを使用してください。 enable password コマンドをテストする可能性があるのは、enable secret コマンドがサポートされないブート モードでデバイスが実行されているときだけです。

enable secret は MD5 アルゴリズムを使用してハッシュ処理されます。 シスコが把握する限り、コンフィギュレーション ファイルの内容をもとに enable secret を復元することは不可能です（明らかな辞書攻撃によるものは除きます）。

注このことは enable secret で設定されたパスワードにのみ適用されます。enable password で設定されたパスワードには適用されません。 実際には、2 つのコマンドの違いは使用されている暗号化の強度が大きく異なることだけです。

enable secret をサポートしている Cisco IOS イメージを調べる方法

通常の運用モード（完全な Cisco IOS イメージ）から show version コマンドを使用してブート イメージを調べ、ブート イメージが enable secret コマンドをサポートしているかどうか確かめます。 サポートしている場合は enable password を削除してください。 ブート イメージが enable secret コマンドをサポートしていない場合は、次の警告に注意してください。

- 物理的なセキュリティを施していてだれもデバイスをブート イメージにリロードできない場合は、enable password の設定が不要になることがある。
- だれかがデバイスに物理的にアクセスできる場合は、ブート イメージにアクセスしなくてもデバイスのセキュリティが容易に破られるおそれがある。
- enable password を enable secret と同じに設定した場合は、enable secret が enable password と同程度に攻撃されやすくなる。
- ブート イメージが enable secret をサポートしていないために enable password を異なる値に設定する場合は、enable secret コマンドをサポートしていない ROM 上でまれにしか使用

しない新しいパスワードをルータ管理者が覚えておく必要がある。 別のイネーブル パスワードを設定すると、管理者はシステムを意図的に停止してソフトウェアをアップグレードする際に（これはブート モードにログインする唯一の理由です）、パスワードを忘れている可能性があります。

その他のパスワード

Cisco IOS コンフィギュレーション ファイル内のほとんどすべてのパスワード、およびその他の認証文字列は、ユーザ パスワードで使用されている脆弱で復元可能な方式を使用して暗号化されています。

特定のパスワードについてどの暗号化方式が使用されているのかを調べるには、コンフィギュレーション ファイル内の暗号化文字列の前にある数字を確かめます。 数字が 7 であれば、パスワードは脆弱なアルゴリズムを使用して暗号化されています。 数字が 5 であれば、パスワードは比較的強固な MD5 アルゴリズムを使用してハッシュ処理されています。

たとえば、次の設定コマンドでは、

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

enable secret が MD5 でハッシュ処理されています。それに対して、次のコマンドでは、

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

パスワードが脆弱で復元可能なアルゴリズムを使用して暗号化されています。

設定ファイル

コンフィギュレーション情報を電子メールで送信するときは、設定からタイプ 7 のパスワードを削除してください。 これには、デフォルトで不適切な情報を削除する show tech-support コマンドを使用できます。 show tech-support コマンドの出力例を次に示します。

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

コンフィギュレーション ファイルを Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）サーバに保存している場合で、コンフィギュレーション ファイルを使用していないときやファイアウォールの背後に配置するときは、コンフィギュレーション ファイルに対する特権を変更してください。

アルゴリズム変更の可能性について

シスコでは、Cisco IOS ユーザ パスワードに対してより強固な暗号化アルゴリズムを近い将来サポートする予定はありません。 将来この機能を導入することをシスコが決定しても、その機能を利用するユーザにとって管理上の負担が増えることは明らかです。

通常の場合、ユーザ パスワードを enable secret で使用されている MD5 ベースのアルゴリズムに切り替えることはできません。これは、MD5 は単方向ハッシュであり、暗号化されたデータからはパスワードをまったく復元できないためです。 特定の認証プロトコル（特に CHAP）をサポートするため、システムはクリアテキストのユーザ パスワードにアクセスする必要があり、そのためそれらのパスワードを復元可能なアルゴリズムを使用して格納する必要があります。

DES などのより強固な復元可能アルゴリズムに切り替える場合、キー管理の問題によって相当の作業が発生します。 DES を使用してパスワードを暗号化するように Cisco IOS を修正すること

は容易ですが、すべての Cisco IOS システムで同じ DES キーを使用するとすれば、そのような修正を加えてもセキュリティ上の利点はまったくありません。 また、システムごとに異なるキーを使用した場合は、すべての Cisco IOS ネットワーク管理者に管理上の負担がかかり、システム間でのコンフィギュレーション ファイルの移植性が失われます。 お客様からも、より強固で復元可能なパスワード暗号化を望まれる声はほとんど頂いていません。

関連情報

- パスワード リカバリ手順
- Cisco IOS デバイスの強化ガイド [英語]
- テクニカルサポート - Cisco Systems