ESA が SSH v2 を使用しているクライアントからの SSH 接続しか受け付けないことを確認するにはどうしたらいいですか?

内容

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス (ESA) 上で SSH 認証バージョンを確認して設定する方法について説明します。

ESA が SSH v2 を使用しているクライアントからの SSH 接続しか受け付けないことを確認するにはどうしたらいいですか?

ESA は、セキュア シェル (SSH) 接続を許可するように設定できます。 SSH 接続は、接続先のホストと ESA 間のトラフィックを暗号化します。これにより、ユーザ名やパスワードなどの認証情報が保護されます。SSH プロトコルには次の 2 つのメジャー バージョンがあります。バージョン 1 (SSH v1) とバージョン 2 (SSH v2) です。より新しい SSH v2 は SSH v1 よりセキュリティが向上しているため、多くの ESA 管理者は優先的に SSH v2 を使用しているクライアントからの接続のみを許可しています。

7.6.3 以前の AsyncOS のバージョンでは、CLI から **sshconfig** を使用して SSH v1 接続を無効にすることができます。

```
mail3.example.com> sshconfig
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings.
[]> setup
SSH v1 is currently ENABLED.
Choose the operation you want to perform:
- DISABLE - Disable SSH v1
[]> DISABLE
```

AsyncOS 8.x 以降のバージョンでは、**sshconfig** を使用して SSH v1 を無効にするオプションが存在しません。 SSH v1 が 8.x のアップグレード前に有効になっていた場合は、アップグレードが

完了して SSH v1 に対するすべてのサポートが削除されたとしても、SSH v1 は ESA 上で有効のまま、アクセスすることができます。このことは、定期的にセキュリティ監査および侵入テストを実施している管理者にとって問題になる場合があります。

SSH v1 のすべてのサポートが削除されているため、サポート リクエストを開いて SSH v1 を無効にしてもらう必要があります。

SSH v1 が問題の ESA に対して有効になっているか無効になっているかを確認するには、外部の Linux/Unix ホストから次のコマンドを実行するか、他の適用可能な CLI 接続を選択します。

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Protocol major versions differ: 1 vs. 2
```

想定される出力は、SSH v1 が無効になっていることを示す "Protocol major versions differ:1 vs. 2" です。 そうではなく、SSH v1 がまだ有効になっている場合は、次のように表示されます。

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Password:
Response:
Last login: Thu Oct 30 14:53:40 2014 from 192.168.0.3
Copyright (c) 2001-2013, Cisco Systems, Inc.

AsyncOS 8.0.1 for Cisco IronPort C360 build 023

Welcome to the Cisco IronPort C360 Messaging Gateway(tm) Appliance
myesa.local>
```

この出力は、SSH v1 がまだ使用中で、8.x 以降にアップグレード後に ESA が安全ではなくなる可能性があることを示しています。 この場合、侵入テストやセキュリティ監査によって注意が喚起され、重大な欠陥が示唆されます。 修正するには、サポート ケースを開いて、この修正を依頼する必要があります。 シスコ テクニカル サポートに対して ESA からのサポート トンネルを提供できる必要があります。

関連情報

- CSCuo46017：アップグレード後に SSHv1 が有効のままになり、無効にできない
- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems