如何確保我的ESA只接受來自使用SSH v2的客戶端的SSH連線？

目錄

簡介

本文檔介紹如何在思科郵件安全裝置(ESA)上稽核和配置SSH身份驗證版本。

如何確保我的ESA只接受來自使用SSH v2的客戶端的SSH連線？

可以將ESA配置為允許安全外殼(SSH)連線。 SSH連線會加密連線主機和ESA之間的流量。這樣可以保護使用者名稱和密碼等身份驗證資訊。SSH協定有兩個主要版本：版本1(SSH v1)和版本2(SSH v2)。SSH v2較新，比SSH v1更安全，因此許多ESA管理員傾向於只允許使用SSH v2的客戶端連線。

在AsyncOS至7.6.3版本中，可以使用**sshconfig**從CLI禁用SSH v1連線：

```
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
```

在AsyncOS 8.x及更高版本中，禁用SSH v1的選項與**sshconfig**不存在。 如果在8.x升級之前啟用了SSH v1，即使刪除了對SSH v1的所有支援，SSH v1仍將保持啟用狀態並可在ESA上訪問。對於執行常規安全稽核和滲透測試的管理員來說，這可能是一個問題。

由於已取消對SSH v1的所有支援，必須開啟支援請求才能禁用SSHv1。

從外部Linux/Unix主機或選擇的其他適用的CLI連線運行以下命令，以確認是否對相關ESA啟用或禁用SSH v1:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
```

```
Protocol major versions differ: 1 vs. 2
```

預期輸出為「協定主要版本不同：1 vs. 2」，表示已禁用SSH v1。 如果未啟用，且SSH v1仍處於啟用狀態，您將看到：

```
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>
```

此輸出將表示SSH v1仍在使用，在升級到8.x或更高版本後，可能導致ESA不安全。 這一點可能會通過滲透測試或安全審計引起注意，並找出一個明顯的差距。 為了進行更正，您需要打開支援案例並請求更正此問題。 您需要能夠從ESA為思科技術支援提供支援隧道。

相關資訊

- CSCuo46017:SSHv1在升級後保持啟用狀態，無法禁用
- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems