停用 ASA 的 SSH 伺服器 CBC 模式密碼

目錄

簡介

本文檔介紹如何在ASA上禁用SSH伺服器CBC模式密碼。在掃描漏洞CVE-2008-5161上，有文檔顯示，在密碼塊連結(CBC)模式下使用塊密碼演算法，使得遠端攻擊者更容易通過未知向量從SSH會話中的任意塊密碼文本中恢復特定純文字檔案資料。

密碼塊鏈是密碼塊的一種運行方式，該演算法使用塊密碼來提供保密性、真實性等資訊服務。

必要條件

需求

思科建議您瞭解以下主題：

- 自適應安全裝置ASA平台架構
- 密碼塊連結(CBC)

採用元件

本文檔中的資訊基於採用OS 9.6.1的Cisco ASA 5506。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

預設情況下，在ASA CBC模式下在ASA上啟用，這可能會成為客戶資訊的漏洞。

解決方案

在增強了CSCum6371之後，在9.1(7)版中引入了修改ASA ssh密碼的功能，但正式包含**ssh密碼加密**和**ssh密碼完整性**命令的版本為9.6.1。

要在SSH上禁用CBC模式密碼，請執行以下步驟：

在ASA上運行「sh run all ssh」：

```
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
```

如果您看到命令**ssh cipher encryption medium**，則表示ASA使用預設在ASA上設定的中高強度密碼。

若要檢視ASA中可用的ssh加密演算法，請運行命令**show ssh ciphers**:

```
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
```

輸出顯示了所有可用的加密演算法： **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。**

要禁用CBC模式以便可以在ssh配置中使用，請使用以下命令自定義要使用的加密演算法：

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

完成此操作後，運行命令**show run all ssh**，現在，在ssh密碼加密配置中，所有演算法僅使用CTR模式：

```
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
```

同樣，可以使用**ssh密碼完整性**命令修改SSH完整性演算法。