排除NCCM 3.8+和CSPC 2.9+中的CBC密碼漏洞

目錄

簡介

本文說明如何對NCCM 3.8+和CSPC 2.9+中的CBC密碼漏洞進行故障排除。

問題

在最新版本的CSPC/NCCM中，我們存在CBC弱密碼漏洞。在大多數情況下，可以通過更新所需的ssh配置檔案來修復此問題。但是，本文被提出來通過加密策略明確拒絕他們的訪問。如果其他所有方法都失敗，則使用此方法。這不會影響預設加密策略，而是在預設策略之上新增額外的層。

傳統方法

確保已從sshd_config中刪除所有CVC密碼。如果問題仍然存在，您可以為/etc/sysconfig/sshd下的引數提供一個空白條目。

```
CRYPTO_POLICY=
```

請確保在執行任何修改之前執行備份。

要驗證此操作是否有效，請在遠端電腦上運行此命令：

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

如果系統提示您輸入密碼或新增RSA金鑰，則問題仍然存在。

解決方案

如果上述過程失敗，您可以通過明確拒絕對CBC密碼的任何訪問來新增額外的加密策略層。我們不建議更改任何加密策略預設配置，因此建議使用此方法。

繼續之前，請確保在預設密碼編譯原則之上未套用其他層。如果有其它層，則可以在進行任何更改之前檢視它們。若要檢查這一點，請運行此命令：

```
update-crypto-policies --show
```

響應為DEFAULT。如果是，則無需任何進一步驗證即可繼續執行後續步驟。

在絕對路徑下建立新檔案：

```
/etc/crypto-policies/policies/modules/DISABLE-CBC.pmod
```

您可以以任何方式命名此檔案，但副檔名以.pmod結尾。

由於我們將刪除此漏洞以使用這些密碼限制ssh訪問，因此請將此行輸入為此新檔案中的唯一條目：

```
ssh_cipher = -AES-128-CBC -AES-256-CBC
```

附註：此專案僅作參考。您可以新增您明確嘗試拒絕的所有密碼，但建議您為除CBC以外的任何密碼建立新檔案，以避免混淆。

儲存檔案後，通過運行以下命令，將crypto-policies的值從DEFAULT設定到此附加層：

```
update-crypto-policies --set DEFAULT:DISABLE-CBC
```

同樣地，DISABLE-CBC值可能因建立檔案時提供的名稱而異。

現在，您可以通過運行以下命令重新檢查：

```
update-crypto-policies --show
```

這一次，它顯示DEFAULT:DISABLE-CBC，確認已新增了一個附加層而沒有修改預設檔案。

在這個階段，如果重新驗證存取，就會遭到拒絕：

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。