

使用本地鏈路AAA伺服器地址的安全訪問RA VPN身份驗證事件

目錄

問題

測試安全訪問遠端訪問(RA)VPN功能時，會為租戶組織中不存在的標識記錄過多的身份驗證事件。身份驗證日誌顯示24小時內超過10,000個RA VPN身份驗證事件，包含AAA錯誤，如「AAALOG_SERVICE_DOWN」和「AAALOG_SERVER_DOWN」。這些錯誤消息引用本地鏈路169.254.x.x地址作為AAA伺服器，這些地址未在租戶中配置。

日誌中觀察到的具體錯誤示例包括：

```
AAALOG_SERVICE_DOWN
AAA authentication server not accessible : server = 169.254.169.79 : user = <user>

AAALOG_SERVER_DOWN
AAA Marking RADIUS server 169.254.169.79 as FAILED
```

本練習似乎是對安全訪問VPN FQDN重複進行基於RADIUS的身份驗證嘗試，從而產生過多的日誌雜訊，並引起對外部掃描或可能濫用VPN服務的擔憂。

環境

- 思科安全存取平台
- 初始配置遠端訪問VPN配置檔案時未進行證書身份驗證
- 為RA VPN配置的基於RADIUS的身份驗證
- 具有可發現VPN配置檔案的公共VPN租戶配置

解析

解決方案涉及瞭解身份驗證流行為以及實施基於證書的身份驗證作為緩解策略。

觀測行為的技術解釋

由於下一節中描述的技術原因，會發生過多的身份驗證事件。

無證書要求的身份驗證流程

當證書身份驗證被禁用且使用基於RADIUS的RA VPN身份驗證時，系統會記錄「授權失敗」嘗試，因為系統首先檢查在Secure Access中同步的使用者資料庫的使用者名稱身份，並記錄「授權失敗」事件。這些事件應作為第一道防線，但在外部參與者嘗試身份驗證時可能會產生嚴重的日誌雜訊。

本地鏈路地址使用情況

日誌中看到的169.254.x.x地址是RA VPN頭端用來授權傳入會話的內部/本地鏈路地址。這些地址表示租戶中的內部系統行為，而不是錯誤配置AAA伺服器。

VPN設定檔探索

配置公共VPN租戶ID時，VPN配置檔案會列在UI下拉選單中，這使得外部參與者可以更輕鬆地發現公共配置檔案並將其作為身份驗證嘗試的目標。

立即緩解步驟

1. — 配置基於證書的身份驗證。修改RA VPN配置檔案以要求基於證書的身份驗證。當需要證書身份驗證時，安全訪問會在身份驗證流程中更早執行證書檢查。如果證書丟失，系統會在標準身份驗證流程之前產生錯誤，並且不會以相同方式記錄「授權失敗」事件。

2. — 驗證緩解的有效性。實施基於證書的身份驗證後監視身份驗證日誌，以確認減少過度身份驗證事件。切換到基於證書的身份驗證成功緩解了攻擊並減少了日誌雜訊。

長期改進

為了解決根本問題，建立了兩個功能請求：

- 功能請求1:新增選項以在新增公共VPN租戶時隱藏或顯示隧道組（VPN配置檔案）清單，從而降低配置檔案的可發現性。
- 功能請求2:新增配置選項以啟用或禁用失敗的RA VPN授權嘗試的日誌記錄，為管理員提供對日誌詳細性的控制。

此外，還會建立一個面向公眾的文檔，解釋記錄的事件和身份驗證行為，以幫助管理員瞭解正常的系統操作。

原因

過多身份驗證事件的根本原因是公共租戶配置中可發現的VPN配置檔案與不需要基於證書的身份驗證時的身份驗證流行為的組合。在沒有證書要求的情況下使用基於RADIUS的身份驗證時，系統會將所有「授權失敗」嘗試記錄為其安全狀態的一部分，包括來自發現VPN配置檔案的外部參與者的嘗試。日誌中的本地鏈路地址代表RA VPN頭端授權過程的正常內部系統行為，而不是配置錯誤。

相關內容

- [思科技術支援與下載](#)

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）。