針對影響遠端訪問VPN服務的密碼噴霧攻擊的最佳實踐

目錄

簡介

本檔案介紹針對針對Cisco安全防火牆上設定的遠端存取VPN(RAVPN)服務的密碼噴霧攻擊而應考慮的建議。

背景資訊

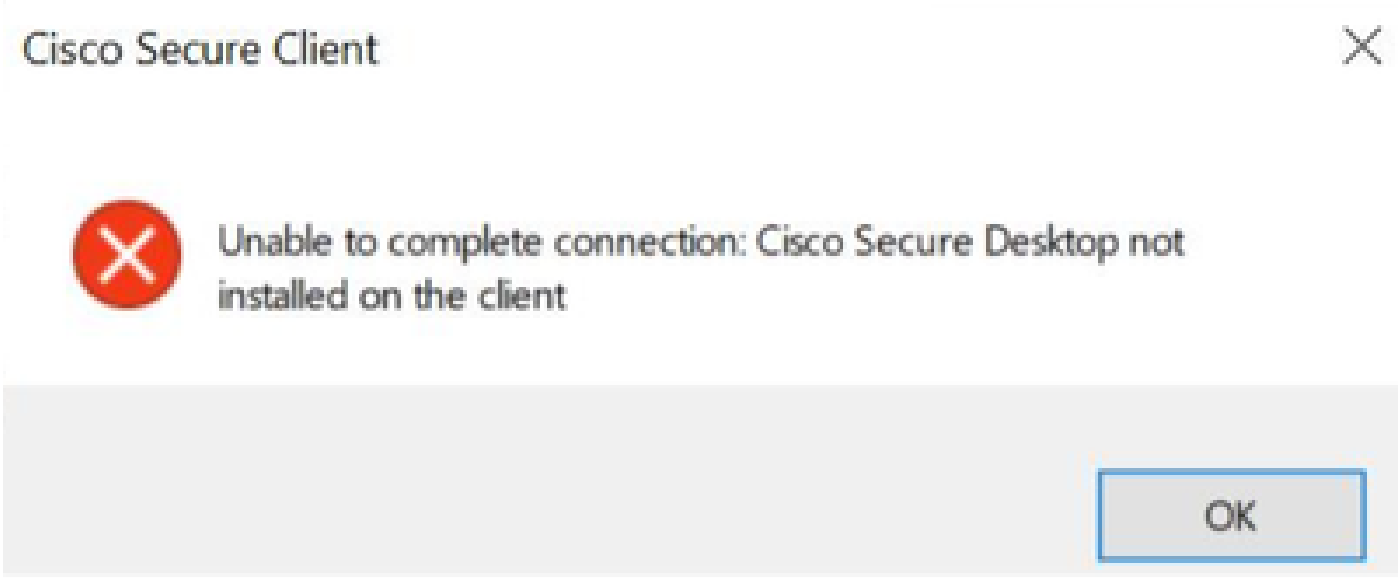
思科獲知多份有關針對RAVPN服務的密碼噴射攻擊的報告。Talos指出，這些攻擊不僅限於思科產品，還包括第三方VPN集中器。

此活動似乎與偵察工作有關。

觀察到異常模式

啟用防火牆狀態(HostScan)時，無法與思科安全客戶端(AnyConnect)建立VPN連線

嘗試使用Cisco Secure Client(AnyConnect)連線時，使用者會收到錯誤「Unable to complete connection（無法完成連線）」。客戶端上未安裝Cisco Secure Desktop。"導致無法成功建立VPN連線。



此症狀似乎就是這些攻擊的副作用；進一步的內部調查仍在進行中。

注意：僅在頭端配置了防火牆狀態(HostScan)的情況下觀察到此特定行為。

異常數量的身份驗證請求

VPN頭端思科安全防火牆自適應安全裝置(ASA)或威脅防禦(FTD)顯示密碼噴霧攻擊的症狀，身份驗證嘗試數達10萬或數百萬次被拒絕。

檢測此情況的最佳方法是檢視系統日誌。查詢任何下一個ASA系統日誌ID的異常數量：

- %ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database :

user

= *admin* : user

IP

= *x.x.x.x*

- %ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

- %ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.

在ASA上配置no logging hide username命令之前，始終隱藏使用者名稱。

注意：這將提供深入資訊，以便瞭解是否生成了有效的使用者，或通過有問題的IP知道有效的使用者，但是，請注意在日誌中將顯示使用者名稱。

要驗證，請登入到ASA或FTD命令列介面(CLI)，運行show aaa-server 命令，並調查嘗試和拒絕的任何已配置AAA伺服器的身份驗證請求的不尋常數量：

<#root>

```
ciscoasa# show aaa-server

Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time 0ms

Number of authentication requests 8473575 - - - - - >>>> Unusual increments


Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
```

Number of rejects 8473574 - - - - - >>>> Unusual increments

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
```

Number of authentication requests 2228536 - - - - - >>>> Unusual increments

```
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
```

Number of rejects 2225363 - - - - - >>>> Unusual increments

```
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

行動

下面列出的操作是建議如何應對針對思科安全防火牆裝置的這些攻擊的影響：

1.啟用日誌記錄

日誌記錄是網路安全的重要組成部分，它涉及記錄系統中發生的事件。由於沒有詳細的日誌，在理解上存在差距，妨礙了對攻擊方法的清晰分析。建議您啟用遠端系統日誌伺服器日誌記錄，以改進各種網路裝置上的網路和安全事件的關聯和稽核。

有關如何配置日誌記錄的資訊，請參見以下特定於平台的指南：

Cisco ASA軟體：

- 使用指南保護ASA防火牆
- Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide中的日誌記錄一章

Cisco FTD軟體：

- 透過 FMC 設定 FTD 中的記錄
- Cisco Secure Firewall Management Center Device Configuration Guide的Platform Settings一章中的Configure Syslog部分
- 在Firepower裝置管理器中配置並驗證系統日誌
- 適用於Firepower設備管理器的Cisco Firepower威脅防禦配置指南的系統設定一章中的配置系統日誌記錄設定一節

2.安全預設遠端訪問VPN配置檔案

如果未使用預設遠端訪問VPN連線配置檔案/隧道組DefaultRAGroup和DefaultWEBVPNGroup，建議使用這些預設連線配置檔案/隧道組，通過將它們指向入孔AAA伺服器來阻止身份驗證嘗試和遠端訪問VPN會話建立。為此，請執行以下步驟：

1.配置虛擬輕型目錄訪問協定(LDAP)伺服器，如下例所示：

```
<#root>

aaa-server

 AAA_Sinkhole

protocol ldap
```

> 注意：請勿新增此AAA伺服器的任何其他配置。

2.將DefaultRAGroup 和DefaultWEBVPNGroup指向此虛擬LDAP伺服器，如下例所示：

```
<#root>

tunnel-group

 DefaultWEBVPNGroup
```

```
general-attributes

authentication-server-group
 AAA_Sinkhole

tunnel-group
 DefaultRAGroup
general-attributes

authentication-server-group
 AAA_Sinkhole
```

注意：如果在預設組重定向到AAA_Sinkhole伺服器後，攻擊者以合法連線配置檔案（隧道組）為目標，則必須阻止這些連線嘗試。請參考後續部分瞭解更多詳細資訊。

3.阻止來自惡意源的連線嘗試

為了阻止來自未授權源的連線嘗試，您可以實施下列任一選項：

注意：最初，您必須檢視安全日誌（系統日誌）以確定有問題的IP地址。識別後，可以使用這3個選項中的任何選項來阻止它們。

注意：必須手動指定和維護要阻止的IP地址清單。

實作介面層級ACL

在ASA/FTD上實施介面級ACL以過濾未授權的公共IP地址並防止它們啟動遠端VPN會話。

使用「shun」命令

這是一種阻止惡意IP的簡單方法，但必須手動完成。有關更多詳細資訊，請閱讀使用「shun」命令阻止安全防火牆攻擊的備用配置部分。

配置控制範圍ACL

在ASA/FTD上實施控制平面ACL以過濾未授權的公共IP地址並防止它們啟動遠端VPN會話。 為安全防火牆威脅防禦和ASA配置控制平面訪問控制策略。

對RAVPN使用基於證書的身份驗證（可選）

與使用憑證相比，使用憑證進行驗證可提供更穩健的方法。要加固環境，可以將RAVPN的身份驗證方法更改為基於證書。

有關詳細資訊，請檢視《思科安全防火牆配置指南》中的配置遠端訪問VPN的AAA設定部分。

其他資訊

- 適用於急救人員的Cisco ASA法證調查程式
- 適用於第一響應者的Cisco Firepower威脅防禦法證調查程式

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）。