採用IPS阻止設定的Cisco安全訪問警告操作覆蓋行為

目錄

問題

在啟用了IPS的Cisco Secure Access上測試訪問策略(Internet Access)中的警告行為時，使用者會遇到意外行為，其中「警告」操作似乎會覆蓋IPS阻止設定。具體而言，當訪問用於觸發IPS簽名的URL時(SERVER-WEBAPP /etc/passwd檔案訪問嘗試， GID-SID:1-1122)，系統會顯示警告頁面，並在使用者確認後，即允許存取URL，而不管已設定IPS以封鎖流量。

配置包括：

- Action:隔離
- 入侵防禦(IPS):啟用
- IPS/阻止
- 簽名：SERVER-WEBAPP /etc/passwd檔案訪問嘗試
- GID-SID:1-1122

活動搜尋日誌顯示衝突條目：

- IPS:(IPS:封鎖)
- WEB:(WEB:允許 — 顯示警告頁面)
- WEB:(WEB:允許（在警告訪問後）

環境

- 產品:思科安全網際網路接入優勢

- 技術：安全訪問
- 配置了Internet Access和Warn操作的訪問策略
- 啟用了IPS，並對特定簽名執行阻止操作

解析

此行為在Cisco Secure Access中被識別為缺陷，其中Access Policies中的Warn操作優先於IPS塊設定。該問題會影響訪問策略警告操作和IPS阻止功能之間的互動。

驗證步驟

要在您的環境中驗證此行為，請執行以下操作：

步驟 1:使用警告操作配置訪問策略並啟用IPS阻止

- 設定要隔離的操作並發出警告
- 啟用入侵防禦(IPS)
- 使用阻止操作配置IPS
- 應用特定簽名(例如SERVER-WEBAPP /etc/passwd檔案訪問嘗試、GID-SID:1-1122)

步驟 2:通過訪問觸發IPS簽名的URL來測試配置

```
https://example.com/etc/passwd
```

步驟 3:觀察行為

- 向使用者顯示警告頁面
- 使用者在確認警告後可以繼續
- 儘管IPS阻止配置，仍允許訪問URL

步驟 4:檢查活動搜尋日誌

- 驗證IPS阻止和WEB允許條目是否存在
- 確認存在衝突的日誌條目指示該缺陷

當前狀態

此行為已被確認為缺陷，其中Warn操作會根據當前實施中的設計覆蓋IPS塊設定。除GID-SID之外的IPS特徵碼會出現相同行為：1-1122，表示這是系統性問題，在配置警告操作時會影響所有IPS簽名。

此缺陷的修正計畫和時間表尚未確定。遇到此問題的組織應評估其安全策略，並在需要嚴格IPS阻止時考慮替代配置。

原因

根本原因是Cisco安全訪問中的缺陷，其中訪問策略警告操作處理優先於IPS塊實施。此設計缺陷允許使用者通過警告確認機制繞過IPS安全控制，從而在配置警告操作時有效地使IPS阻止功能無效。

思科錯誤ID CSCwt39270與此案件相關，雖然此錯誤與已觀察到的警告與IPS行為之間的特定關係需要進一步調查。

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）。