

沒有資料分類的安全訪問DLP檔案大小規則不會生成文本檔案的監控器事件

目錄

問題

僅使用檔案大小條件配置的Cisco Secure Access Web DLP策略（無資料分類）不會為.txt檔案上傳生成DLP監控事件，而同一策略會為其他檔案型別（如.xlsx、.png和.pdf檔案）正確觸發監控事件。受影響的策略Advanced Management Policy - Web配置有：

- 自定義檔案大小在1KB和49MB之間的檔案控制
- 無資料分類標準
- 設定為「監控」的操作

測試顯示：

- Action = Monitor時，TXT檔案上傳不會顯示在DLP事件中。
- 當Action = Block時，相同的TXT檔案會正確生成DLP事件。
- 活動日誌顯示包括TXT檔案在內的所有檔案上傳。
- 其他檔案格式(PNG、PDF、XLSX)會使用「監視器」(Monitor)操作按預期生成DLP事件。

此外，在DLP規則中未配置資料分類時，無論配置的規則嚴重性設定如何，記錄的DLP事件始終顯示Medium嚴重性。

環境

- 思科安全存取（前身為Cisco Umbrella）
- DLP（資料丟失防護）Web策略

- 啟用HTTPS解密的Internet訪問策略
- 通過Web應用程式執行的檔案上傳測試

解析

這種行為沒有記錄，但設計上是預期的。當使用僅檔案大小條件和Monitor操作來防止日誌過載時，會繞過DLP監視中的MIME型別（如text/plain）。開發團隊證實，這是沒有外部記錄的故意行為。

解決方法選項

選項1（推薦）：新增資料分類

在DLP規則中新增任何廣泛的資料分類標準，同時保留Action = Monitor。

此恢復：

- TXT檔案DLP事件生成
- 根據規則配置更正嚴重性處理

選項 2:將操作更改為阻止

將規則操作從Monitor更改為Block。這會為TXT檔案生成DLP事件，但也會強制實施僅監控使用案例所不能使用的阻止。

實驗室測試結果

全面的實驗室測試證實了行為模式。

測試場景1:具有資料分類和檔案大小的DLP規則(1KB-49MB)，操作=塊

- TXT檔案和PII:已阻止和已記錄
- PDF檔案：已阻止和已記錄
- 不帶PII的TXT檔案：允許（預期）
- 使用PII的PNG:允許（基於分類而預期）

測試場景2:僅具有檔案大小的DLP規則（無資料分類），操作=塊

- 所有檔案型別（TXT、PDF和PNG）：已阻止和已記錄
- 嚴重性顯示為Medium，儘管規則配置為Low

測試場景3:僅具有檔案大小的DLP規則（無資料分類），操作=監視器

- TXT檔案：允許但未登入DLP事件
- PDF和PNG檔案：允許並登入DLP事件
- 活動日誌顯示所有上傳，包括TXT檔案

原因

這是Cisco Secure Access DLP中故意但未記錄的行為。當使用僅檔案大小規則和Monitor操作來防止生成過多的日誌時，系統會繞過text/plain MIME型別的DLP事件記錄。行為與操作相關，並且特定於MIME型別：

- 使用僅檔案大小條件監控操作：通過日誌記錄繞過的TXT檔案
- 使用僅檔案大小條件阻止操作：正常記錄的TXT檔案
- 存在資料分類的任何操作：正常記錄的TXT檔案

出現嚴重性問題的原因是，在內容感知模式下運行時，DLP事件從資料分類後設資料而不是規則設定獲取嚴重性。如果不使用Data Classification (資料分類)，無論配置的規則嚴重性如何，系統都會預設為「Medium」(中) 嚴重性。

相關內容

- [Cisco Secure Access DLP檔案大小配置](#)

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）。