# 誤報變少之後：讓憑證警示的判讀有據可查

2026-11-28 · 8plus

GitHub 於 2026 年 11 月 23 日宣布改善 Slack 憑證掃描：針對 slack_incoming_webhook_url，排除不符合 Slack incoming webhook 網址格式的比對結果。這是一項特定偵測器的誤報改善，不代表所有警示都經過有效性驗證，也不代表專案已沒有外洩風險。

## 警示數量不是驗收結論

以下是 8plus 的交付建議，不是漏洞事件或成效實測。工具更新後，警示變少可能來自辨識規則變精準，不能直接解讀成團隊修好了同樣數量的問題。若要比較前後狀態，應同時記錄掃描範圍、規則變更與處理進度。

把「發現多少」與「確認多少」分開。候選字串需要核對來源與用途；確定的事件需要處理；資訊不足的項目應保留待查。三者若都被算成已解決，儀表板會很漂亮，下一位接手的人卻不知道還剩什麼。

## 留下判斷理由，而不是複製秘密

一筆可交接的紀錄，可以包含警示識別碼、受限存取的來源位置、負責人、判斷理由與下一步。不要把完整 webhook 或憑證貼進公開 issue、聊天摘要或分析事件；紀錄本身不應成為另一個外洩位置。

若判定為測試資料，應能說明它為何不是可用的正式秘密；不能只因檔名包含 test 就關閉警示。無法確認時，標記待查並交由有權限的人處理，不要以猜測補齊狀態，也不要為了驗證而任意對外發送請求。

## 把關閉警示與處理憑證分開

關閉一筆通知只是工作流程的狀態變更。若確認有效憑證已暴露，應依服務商與組織流程撤銷或輪替，檢查受影響的使用端，再記錄處置結果。刪除最新檔案中的字串，不能替代對憑證本身的處理。

交付時也要說清楚責任邊界：誰能判讀、誰能輪替、誰確認服務恢復。不要讓一位只能看見掃描結果的人，被默認成已完成所有修復。必要的權限與復原步驟應事先確認，避免臨時處理時中斷服務。

## 用小型交接檢查守住結尾

每輪整理後，抽查已處理與待查項目，確認理由、負責人及下一步仍可找到。報告只呈現必要的彙總與受控連結；不把秘密值傳入 GA 或其他網站分析工具。

誤報降低能節省閱讀時間，但省下來的注意力應用在真正需要判斷的地方。好的安全交付不是把數字清成零，而是讓下一個人看得懂：哪些已處理，哪些仍未知，以及接下來由誰確認。

## 來源

官方公告

延伸閱讀