

Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-24-010

Openfind 郵件安全威脅與潛在資安風險通報

Openfind 專注於郵件安全領域已經有 25 年以上的豐富經驗，致力提供客戶穩定、安全、可靠的郵件安全系統與服務。為提昇客戶郵件安全意識與避免潛在資安風險擴大，Openfind 郵件安全研究團隊將不定期提供客戶有關郵件安全威脅的即時訊息，以及潛在資安風險的警示通報。

如果您在使用 Openfind 各項產品時，有發現任何郵件安全威脅或潛在資安風險，也歡迎您透過 support@openfind.com.tw 與我們聯繫。Openfind 技術團隊將提供您即時的資安諮詢與更新服務。

公告日期：2024/10/16

威脅類別：Improper Input Validation（未驗證不當輸入）

威脅程度：3（分數 1~5，5 代表資安事件威脅程度很高）

影響產品版本：Mail2000 v7.0

事件摘要：

近日 Openfind 電子郵件威脅實驗室分析存取紀錄，發現有攻擊者盜取使用者權限後，透過複合式手法利用 CGI 未驗證不當輸入的弱點進行攻擊。輸入驗證是一種常用技術，用於檢查潛在危險的輸入，以確保輸入對於在代碼內部處理或與其他套件間的通訊是安全的。當軟體未正確驗證輸入時，攻擊者可以以應用程式未預期的形式製作輸入。這將有機會造成系統接收意外輸入，以導致控制流程變更、資源的任意控制或任意代碼執行。

建議措施：

目前網擎雲端服務如 MailCloud、EaaS 環境等已全數更新，建議所有 Mail2000 v7.0 軟體客戶立即以 Openfind 官方所提供的安全性修正程式更新系統，以阻絕任何潛在風險。

更新方式：

針對 Mail2000 客戶，可透過兩種方式來進行漏洞修補的更新，您可聯繫 Openfind 技術服務團隊，以協助進行更新事宜或使用產品線上更新功能，自行進行更新。

- **Mail2000 標準版 v7.0 客戶請由 [線上更新] 頁面更新。**
請由線上更新頁面，依序更新 Patch 至 v7.0 第 136 包。
更新方式請參考：[管理者介面更新操作手冊](#)。

- Mail2000 客製版客戶請先確認系統版本並提供系統版號給網擎資訊技術人員，由網擎資訊技術人員提供安全性程式更新包。

系統版號位置：「管理介面 > 系統 > 系統資訊 > 更新資訊」中查找最新日期之編號。



系統資訊	
產品名稱：	Mail2000 Message System
產品版本：	Mail2000 V80
授權期限：	2026/01/19 11:14:07

更新資訊	
mp802404021605	2024/04/13 11:18:06
mp802403141055	2024/04/13 11:16:25
mp802403111748	2024/04/13 11:11:57
Sophos 607	2024/03/21 10:39:54
Sophos 606	2024/03/20 07:44:05

關於 Openfind 電子郵件威脅實驗室

隨著資訊安全威脅日益升高，所有資訊系統都面臨相當嚴峻的挑戰。其中，電子郵件系統更是諸多資安威脅中首當其衝的主要標的。由於資訊安全的範圍相當廣泛與多元，在實際的案例中，客戶只需要定期更新 Patch 與升級系統，結合 Openfind 主動式安全偵測服務，便可避免暴露於風險之中。Openfind 本著服務客戶的精神，不但會繼續強化產品在資安上的防護與感知能力，也會持續嚴格監控產品的安全。Openfind 電子郵件威脅實驗室也會不定期更新網路上重大的電子郵件安全威脅訊息，幫助管理者掌握最新的資安趨勢與脈動。