

Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-22-008

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 20 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：2022 / 12 / 13

威脅類別：複合式攻擊

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、V8

事件摘要：

近日 Openfind 接到 BCCS 漢昕科技 Lin HanChao 通報，攻擊者在竊取使用者帳號密碼並登入系統後，若該被竊取之帳號具有公共空間的寫入權限，則可透過在空間中上傳含有 XSS (跨站腳本攻擊，Cross-Site Scripting) 的惡意檔案，再以其它方式成功誘使同系統其它帳號開啟該檔案後，可能取得其它帳號之登入階段認證，危害帳號與系統安全。

Openfind 開發團隊已於第一時間回應通報並提供安全性修正程式 (Security Patch)。

建議措施：

建議所有 Mail2000 產品客戶立即更新至產品最新版，以阻絕任何潛在性風險。請使用 Mail2000 管理介面中的產品線上更新功能，可將系統自動更新至最新版。如有問題，亦歡迎聯繫 Openfind 技術服務團隊或洽詢您的經銷商窗口，我們將協助您進行更新事宜。

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。