Openfind Software Engineered for Growth

Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-20-011

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：2020 / 10 / 21

威脅類別：安全性強化與宣導

威脅程度：0（分數 1~5，5 代表資安事件威脅程度很高）

影響產品版本：Mail2000 客戶

事件摘要：面對國家級駭客攻勢 Openfind 呼籲管理者盡速更新 Patch 以確保系統安全

2020 是動盪不安的一年，延續美中貿易戰衝突局勢升高，再伴隨新冠疫情蔓延全球，近期再加上美國大選影響，讓國家級駭客躍躍欲試進而竊取機密資料，近期包含美國、澳洲、德國也陸續傳出受駭災情。而台灣亦遭受國家級駭客猛烈攻擊更勝以往，不僅是政府單位，包括高科技製造業與半導體業者也承受針對式進階持續攻擊。然而，駭客在竊取特權帳號過程中，最常利用電子郵件來進行，因此相較以往 Mail2000 近期也承受較多次且手法更進階的資安威脅，以 Mail2000 的客戶屬性與市佔率，此類資安事件發生於政府機關尤占多數。

Openfind 所有的產品及雲端服務皆為自主研發、自行維運，搭配累積多年研發之各式監控機制，主動偵測到異常資料及連線行為並隨即阻擋。深入近期事件調查後發現，此為來自中國網軍以電子郵件簽名檔嵌入 CSRF 手法、並結合儲存型 XSS 的組合式攻擊。針對此事件，Openfind 主動通報包括各機關、各級單位與民間企業，呼籲所有系統管理者立即進行更新，若您有任何更新上的疑慮，研發團隊將協助您透過管理介面更新至最新 Patch、停止使用 IE11 改用支援最新資安規範的瀏覽器，如 Chrome、Firefox 或最新版 Edge，亦可有效防制未來潛在的資安問題。

Openfind 於 2009 年通過 ISO27001 資安認證至今，於產品開發時嚴格遵循 SSDLC（Secure Software Development Life Cycle）程序，全力防護客戶系統安全、以最新技術抵禦攻擊，並積極研發主動偵測及警示手段，緊盯各種可疑狀況、主動通報，懇請各機關單位與網擎共同聯防，以達到防禦縱深與資安防護等級的提升。若您對郵件安全有任何疑問，請聯繫 support@openfind.com.tw