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-24-007

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 / 06 / 20

威脅類別：CGI 漏洞與複合式攻擊

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：MailGates V6.0、MailAudit V6.0、Mail2000 V7.0、Mail2000 V8.0

事件摘要：

根據外部情資，本公司產品經查證確認後發現以下潛在風險，因此主動釋出相應的安全性修正程式（Security Patch）。

MailGates 與 MailAudit（皆為 V6.0 版本）：

- 提升 Cookie（存在於網頁用戶端的資訊）機制安全性，將啟用 HttpOnly 標籤以防止客戶端腳本（例如 JavaScript）存取 Cookie 的內容。
- 修正潛在安全弱點，提升系統安全性。

Mail2000（V7.0 與 V8.0 版本）：

- 當通過帳號授權使用 IMAP4 服務時，修正在特定操作下可能會觸發堆疊溢位（Stack Overflow）漏洞所導致潛在的安全性問題。IMAP4（Internet Message Access Protocol Version 4）是一種應提供使用者從用戶端存取電子郵件系統的協定。
- 修正潛在的 XSS 風險。XSS 跨站腳本攻擊（Cross-site scripting 的簡稱或是稱為跨站指令碼攻擊）是一種網站程式的安全漏洞攻擊。此漏洞允許攻擊者將自身的惡意程式碼注入網頁當中，遭

受攻擊後，一般使用者可能在不知覺的情況下被盜取 Cookie 資訊、帳號身份因而遭盜用，可能會有信件等個人資料被竊取之風險。

- 修正 Cookie 啟用 HttpOnly 標籤後客戶端腳本（例如 JavaScript）相關問題。

建議措施：

目前網擎雲端服務如 MailCloud 環境已全數更新，建議所有 MailGates、MailAudit 與 Mail2000 產品客戶立即更新至 Openfind 官方所提供的安全性修正程式，以阻絕任何潛在性風險。

更新方式：

MailGates 請使用產品線上更新功能，或可聯繫 Openfind 技術服務團隊協助進行更新事宜。

- **MailGates/MailAudit 標準版客戶請由【線上更新】頁面更新。**
  V6.0 客戶請依序更新 Patch 至 6.1.7.040
  更新方式請參考：管理者介面更新操作手冊
- **MailGates/MailAudit 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，由網擎資訊提供安全性程式更新包。**
  V6.0 客戶請以系統管理者登入，點擊「管理選單 > 系統管理 > 系統升級」，接著選取【MailGates 軟體升級】分頁，即可檢視軟體版本。

Mail2000 請使用產品線上更新功能，或可聯繫 Openfind 技術服務團隊協助進行更新事宜。

- **Mail2000 標準版客戶請由【線上更新】頁面更新。**
  Mail2000 V7.0 & 8.0 客戶：
  請由線上更新頁面，依序更新 Patch 至 V7.0 第 131 包或 V8.0 SP2 第 044 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，由網擎資訊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。

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。