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-24-004

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 / 03 / 14

威脅類別：安全性強化

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、MailGates

事件摘要：

Openfind 電子郵件威脅實驗室於近期發現有攻擊者試圖進行系統攻擊，根據我們長期研究攻擊者的行為並分析的結果，相較於利用零日 (ZeroDay) 攻擊，惡意組織更常應用已公布的漏洞來攻擊尚未更新的系統。因此，此次的定期更新我們除了釋出包含 Mail2000、MailGates 的例行安全性更新及程式升級之外，也透過資安通報建議所有 Mail2000、MailGates 客戶儘速更新至最新版本以保護您的系統，避免非預期的企業損失。

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 Mail2000、MailGates 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，升級步驟請參考下方更新方式說明。

Mail2000 更新方式：

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。

- **標準版：**
  Mail2000 客戶：

  1. 請由線上更新頁面更新：
     - V7 客戶請依序更新 Patch 至 SP4 第 125 包
     - V8 客戶請依序更新至 SP2 第 035 包
  2. 更新方式請參考：管理者介面更新操作手冊。

- **客製版：**

  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。

  ```
  $ cat /webmail/etc/m2kpatch.info
  ```

  例如：

  ```
  mp802304281456   2023/05/11 10:10:46
  mp802305181706   2023/05/24 11:10:12
  ```

MailGates 更新方式：

MailGates 與 MailAudit 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。

- **標準版：**
  - **V5.0 客戶：**請點擊「系統管理> 系統升級」，選取【MailGates/MailAudit 軟體更新】分頁，請依序更新 Patch 至 5.2.10.092 版本。
  - **V6.0 客戶：**請點擊「管理選單> 系統管理> 系統升級」，選取【MailGates/MailAudit 軟體更新】分頁，請依序更新 Patch 至 6.1.07.034 版本。

- **客製版：**
  請以管理者帳號登入 MailGates 或 MailAudit 並進入管理者介面，點入右上角「授權資訊」後，下方「安裝模組」之後的第一行，會顯示您的主機版本及客製版號，請複製類似「mg-6.x.x.xxx」整行字串後提供給網擎資訊，由原廠提供專屬的安全性程式更新包。

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。

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，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。