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-22-003

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 / 05 / 10

威脅類別：OpenSSL 函式庫漏洞（CVE-2022-0778）

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：Openfind Mail2000、MailGates、MailAudit、MailBase 與 SecuShare Pro 各版本

事件摘要：

編號 CVE-2022-0778 的資安漏洞是加密連線所使用之 OpenSSL 舊版函式庫中含有無限迴圈之程式疏漏，可能特殊的連線指令觸發而造成 DoS 阻斷服務，致使伺服器無法正常運作。Openfind 各主要產品因套用 OpenSSL 函式庫故提供各產品修正程式，建議客戶更新各產品版本以降低資安風險。

建議措施：

1. **Openfind Mail2000**

   V7 標準版：請由線上更新頁面，依序更新 Patch 至 SP4 第 111 包或更新版本。

   V8 標準版：請由線上更新頁面，依序更新 Patch 至第 014 包。

   更新方式請參考：管理者介面更新操作手冊。

   客製版：請以下述指令取得版本號提供給技術服務窗口，以專屬 Security Patch 更新系統：

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

   例如：

   ```
   Mp701412221626   2019/11/06 14:41:21
   Mp701412261508   2019/11/06 14:41:51
   ```

2. **Openfind MailGates 與 Openfind MailAudit**

   V5 標準版：請由線上更新頁面，依序更新 Patch 至 5.2.10.071 版本。

   客製版本：請登入 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，

   請將類似「mg-5.x.x.xxx」之整行字串提供給技術服務窗口，以專屬 Security Patch 更新系統。

3. **Openfind MailBase**
   請更新至 mbase.tw_6.2.03.013 或更新版本。

4. **Openfind SecuShare Pro**
   請更新至 SecuShare Pro V3 的 3.3.11 或更新版本。

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。