Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-21-005

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：2021 / 12 / 24

威脅類別：Apache 安全性漏洞 (CVE-2021-44224 與 44790)

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：Openfind 全產品皆不受影響

事件摘要：

近日，Apache HTTP Server 發佈安全性更新（版本 2.4.52），針對安全性漏洞 CVE-2021-44224 與 CVE-2021-44790 進行修復。Openfind 資安團隊已於第一時間確認全產品包含 Mail2000、MailGates、MailAudit、MailBase **均不受漏洞影響**，敬請各位用戶放心。

- CVE-2021-44224 危害等級：中

  由於對用戶輸入驗證不足，攻擊者可透過使用特製的 HTTP 請求導致 httpd 伺服器崩潰（當配置為前置代理時）或進行伺服器端請求偽造攻擊（當配置為混合轉發或反向代理時）。

  Openfind 全產品標準設定下並未使用前置代理 (forward proxy) 及相關 Apache 模組，故不受影響。

- CVE-2021-44790 危害等級：高

  由於 mod_lua 解析 multipart 內容時可能出現緩衝區溢位，攻擊者利用該漏洞可透過精心設計的 HTTP 請求進行緩衝區溢位攻擊。

  Openfind 全產品標準設定下並未使用 mod_lua 模組，故不受影響。

建議措施：

Openfind 全產品客戶無須採取任何措施。

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。