Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-21-002

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 / 07 / 02

威脅類別：Palo Alto Networks 等防火牆設備造成 PDF 信件遭退信

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、MailGates、MailAudit 等產品客戶

事件摘要：

根據客戶回報，自 2021 年 7 月 1 日起，經過 Palo Alto Networks、SonicWall 及 Check Point 等防火牆（Firewall）等設備之 SMTP 連線，若含有 PDF 附檔，有機率該連線會被防火牆設備阻擋，造成退信，退信原因（DSN，Delivery Status Notification）註明為「5.4.1 Content blocked by Internal Firewall」。

經查明因 Openfind 所有相關產品不會回傳此一退信原因（代碼 541），且由於防火牆設備一般會位於網擎 MailGates 與 Mail2000 等設備前端，可以較早影響收發信 SMTP 連線，因此相關的過濾及退信問題，應為防火牆設備之機制影響，並非由網擎的郵件防護系統造成。

建議措施：

建議客戶遇到此類問題，可洽詢防火牆廠商，更新或調整防火牆設備之安全政策等相關設定。

- **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。