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-26-001

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：2026 / 01 / 27

威脅類別：複合式攻擊

威脅程度：4.5 (分數 1~5，5 代表資安事件威脅程度很高)

影響產品版本：MailGates 5.0/6.0、MailAudit 5.0/6.0

事件摘要：

近日 Openfind 電子郵件威脅實驗室研究人員發現，MailGates/MailAudit 系統中的 CGI（Common Gateway Interface）存在緩衝區溢位（Buffer Overflow）安全性漏洞及 CRLF（Carriage Return Line Feed）注入漏洞，可能被利用導致系統檔案遭未授權存取。為降低相關風險，Openfind 資安團隊已於第一時間釋出安全性修補程式（Security Patch），以阻絕潛在攻擊途徑。

建議措施：

目前網擎雲端服務如 MailCloud、EaaS 環境等已全數更新，建議所有 MailGates 與 MailAudit 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 與 MailAudit 客戶可透過兩種方式來進行漏洞修補的更新，第一種是聯繫 Openfind 技術服務團隊，以協助進行更新事宜；另一種則是使用產品線上更新功能，自行進行更新。

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 6.1.10.054
- v5.0 客戶請依序更新 Patch 至 5.2.10.099
- 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，你可檢視軟體版本。

- v5.0 客戶請以系統管理者登入，點擊「系統管理 > 系統升級」，接著選取【MailGates 軟體升級】分頁，你可檢視軟體版本。

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。