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-20-003

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：2020 / 04 / 14

威脅類別：LDAP 驗證加密

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、MailBase、ArkEase Pro 產品客戶

事件摘要：

根據「Microsoft ADV190023 適用於啟用 LDAP 通道繫結和 LDAP 簽署的 Microsoft 指引」中提到「預計未來將進一步在 2020 年下半年發行每月更新使用預設值設定，啟用網域控制站上的 LDAP 簽署和通道繫結」，Microsoft 建議將針對 Active Directory 網域控制站上的 LDAP 通道繫結和 LDAP 簽署使用新的預設設定，取代原始不安全的設定，提升 Microsoft 產品的安全性。

Openfind 所有相關產品並無此安全性問題，唯因常與該 Microsoft 系統整合，基於善意提醒發布此通報。Openfind 開發團隊已於 2020 年 3 月，提供各產品修正程式（Patch）及解決方法。

建議措施：

建議所有 Openfind 產品客戶更新至 Openfind 官方所提供的最新版修正程式，並於 LDAP 相關設定（如登入驗證、群組同步等）項目中，啟用 SSL/TLS 以提升 LDAP 驗證安全性。

更新方式：

請點選下列對應產品名稱，參考網擎資訊技術支援中心內詳細說明

- Mail2000 (標準版)
- Mail2000 (客製版)
- MailGates、MailAudit (標準版)
- MailGates、MailAudit (客製版)

- MailBase (標準版)
- ArkEase Pro (標準版)

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。