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-21-004

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 / 16

威脅類別：Apache Log4j（CVE-2021-44228）

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：

為提供客戶穩定、安全、可靠的郵件安全系統與服務，Openfind 電子郵件威脅實驗室長期主動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。編號 CVE-2021-44228 的漏洞發生於開源日誌資料庫 Log4j。Log4j 的 JNDI 功能可用於組態、紀錄訊息，包含於許多軟體專案中，包括 Apache Struts2、Apache Solr、Apache Druid、Apache Flink 等，Log4Shell 漏洞影響 Log4j 2.0-beta-9 和以上版本，以及 2.14.1 和以下版本。Apache 基金會已釋出更新版本 2.15.0 版。詳細請參閱：Apache 基金會。

Openfind 全產品包含 Mail20000、MailGates、MailAudit、MailBase、ArkEase Pro、MailCloud Messenger 及 Openfind Enterprise Search（OES）**均不受 Log4j 漏洞影響**，敬請各位用戶放心。

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。