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-19-009

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：2019 / 12 / 12

威脅類別：安全性強化

威脅程度：1 (分數 1~5，5 代表資安事件威脅程度很高)

影響產品版本：Openfind Enterprise Search 4.0, 4.5 及 4.6 產品版本

事件摘要：

搜尋引擎在企業網站的主要應用，是藉由網頁上提供的搜尋框，讓網站訪問者透過關鍵字查找，更快進入目標網頁，以獲得相關的資訊或下載資料，增加網站瀏覽的效率。

為達成此一目的，通常搜尋引擎會事先以網路爬蟲 (Crawler) 的機制，採用類似瀏覽器訪問方式，將提供給一般使用者瀏覽或訪問的資料進行整理，使得搜尋時可以加快回應的速度。

Openfind 經資安團隊通知，於 OES 近期版本中，使用者可能可以透過其它方式，不經由正常搜尋後訪問或下載的流程，而能直接取得相關的資訊。此方式雖然不會造成重大風險，但為避免網站管理的困擾, Openfind 已經主動提供相關修正程式 (Patch) 來強化安全性。

建議措施：

建議 OES 4.0/4.5/4.6 的客戶安裝修正程式，以強化系統安全並阻絕潛在風險。如仍使用舊版 OES 的客戶，建議進行升級規劃，此部分請洽 Openfind 業務；其它有關更新問題，歡迎透過 support@openfind.com.tw 或來電 (02)2553-2000 與我們聯繫。

更新方式：

Openfind OES 產品之客戶，可按照下列方式進行進行更新，或透過聯繫 Openfind 技術服務團隊，以協助進行更新事宜。

（1）. **停止 ORIS Index Server 及 ORIS Web Server 服務**
- 請先確認 OES 沒有在建索引，若有，請待索引建立完成後再行更新檔案。
- 停止服務方式可參考 Windows 服務操作方式。
- 若有使用 IIS，請一併停止 IIS 服務。

（2）. **下載及更新 OES 安全性更新檔案**
- 請依所使用的版本，下載相對應的 Patch。下載路徑為 https://www.openfind.com.tw/taiwan/resource.html, “Search 產品線 “
- 備份原有檔案。(路徑：OES 安裝目錄\OES\orishttp 及 OES 安裝目錄\OES\search)
- 將下載的檔案解壓縮後，複製至相對應的路徑。

（3）. 啟動 ORIS Index Server 及 ORIS Web Server 服務
- 重新啟動方式可參考 Windows 服務操作方式
- 若有使用 IIS，請一併啟動 IIS 服務。

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。