Openfind Software Engineered for Growth

Openfind 資訊安全威脅與潛在資安風險通報

編號：OF-ISAC-18-005

Openfind 資訊安全威脅與潛在資安風險通報

Openfind 專注於資訊安全領域已經有 20 年以上的豐富經驗，致力提供客戶穩定、安全、可靠的資訊安全系統與服務。為提昇客戶資訊安全意識與避免潛在資安風險擴大，Openfind 資訊安全研究團隊將不定期提供客戶有關資訊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，有發現任何資訊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：2018 / 7 / 25

威脅類別：CGI 漏洞

威脅程度：2 (分數 0~5，5 代表資安事件威脅程度很高)

影響產品版本： Openfind Enterprise Search 3.0 SP2 及 4.0 產品客戶

事件摘要：

CGI（Common Gateway Interface）為現今網站普遍應用的重要網路技術，可以透過網頁瀏覽器對網站伺服器提供請求，而網站伺服器會針對該請求進行相對回應。此一 CGI 漏洞須透過相當罕見的攻擊手法，利用極難發現的緩衝區溢位之途徑入侵；該手法屬於相當進階且需要耗費大量時間才能計算出入侵點之攻擊手法，截至目前為止，尚未發現任何客戶單位實際遭此方式攻擊，因此尚未造成影響。目前 Openfind 已經主動提供安全性修正程式（Security Patch）與解決方法，以便協助客戶儘速處理。

建議措施：

建議 OES 3.0 SP2 及 4.0 產品客戶立即安裝安全性修正程式，以確保系統安全並阻絕潛在風險。如有任何相關問題，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。

關於 Openfind 資訊安全威脅實驗室

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，資訊安全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 資訊安全威脅實驗室也會不定期更新網路上重大的安全威脅訊息，幫助管理者掌握最新的資安趨勢與脈動。