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-19-002

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 / 01 / 16

威脅類別：CGI 漏洞與 XSS 攻擊

威脅程度：3（分數 1~5，5 代表資安事件威脅程度很高）

影響產品版本：Mail2000 7.0 產品客戶

事件摘要：

- CGI（Common Gateway Interface）
  是一重要且現今網站普遍應用的網路技術。此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。Openfind 日前發現當透過正常的使用者帳號密碼登入 Mail2000 後，在特定方法下能讀取到不合法資料，產生安全性問題。

- XSS 跨站腳本攻擊（Cross-site scripting 的簡稱或是稱為跨站指令碼攻擊）
  是一種網站程式的安全漏洞攻擊。此漏洞允許攻擊者將自身的惡意程式碼注入網頁當中，遭受攻擊後，一般使用者可能在不知覺的情況下被盜取 Cookie 資訊（存在於網頁用戶端的資訊）、帳號身份因而遭盜用。

Openfind 在發現漏洞後已於第一時間主動提供安全性修正程式（Security Patch）與解決方法，並協助客戶儘速更新，包括此次威脅在內的許多資安風險皆始於帳號密碼被他人取得，建議使用以下 Mail2000 提供的安全措施，保護最基本也是最重要的帳號安全：密碼原則設定、OTP 雙重認證、限制登入 IP 或開啟異常登入警示、使用 HTTPS、TLS 加密通道。另外，Mail2000 於 7.0 版後已於最易受攻擊的讀信功能加入 Content-Security-Policy（以下簡稱 CSP）規格，因此只要使用較新版本之瀏覽器如：Chrome、Firefox 及 Edge 等，即可防止 XSS 跟網頁樣式置換攻擊，不需額外擔心。但目前 IE 瀏覽器不在 CSP 支援範圍內。

建議措施：

建議所有 Mail2000 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：

針對 Mail2000 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。

- **標準版：**
  Mail2000 V7.0 客戶：
  請由線上更新頁面，依序更新 Patch 至 SP4 第 065 (190115) 包。
  更新方式請參考：管理者介面更新操作手冊。

- **客製版：**
  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。

```
$ cat /webmail/etc/m2kpatch.info
```

例如：

```
mp601412221626   2018/01/06 14:41:21
mp601412261508   2018/01/06 14:41:51
```

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。