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-21-001

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 / 2 / 3

威脅類別：XSS 跨站腳本攻擊

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

事件摘要：

Openfind 電子郵件威脅實驗室於 2 月初發現 XSS 跨站腳本攻擊事件，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，發現事件後，Openfind 電子郵件威脅實驗室於第一時間進行修補並提供安全性程式更新包。

行政院資安處面對政府單位不斷受到資安攻擊的挑戰，於 2017 年起持續推動 8 大「資安旗艦計畫」，其中，政府推動組態基準（Government Configuration Baseline, GCB）目的即是為了有效降低惡意行為的入侵管道，避免產生資安事件的疑慮。有鑑於此，Openfind 為服務廣大的政府及企業用戶，針對資安議題專程提供了 Mail2000 電子郵件政府組態基準（簡稱 Mail2000 for GCB），讓使用 Mail2000 系統的政府機關及企業可獲得最完整且具系統性的資安防護設定，詳細資訊請參考下方建議措施。

建議措施：

建議所有使用 Mail2000 7.0 的客戶，立即更新安全性修正程式，以阻絕此潛在性風險。另外，Mail2000 系統本身也另有多項安全性相關之功能，也建議客戶設定開啟，以加強系統安全。

- 系統 / 環境設定 / 安全性功能設定 / Session 檢查 IP：開啟

● HttpOnly（經由底層 conf 開啟）

```
/webmail/etc/openfind.conf
HTTPONLY_ENABLE=1
```

●其他資安詳細設定亦可於網擎資訊軟體股份有限公司之線上手冊查閱：

https://openfind.tw/R/GCB

更新方式：

- **標準版：**
  Mail2000 V7.0 客戶：
  請由線上更新頁面，依序更新 Patch 至 SP4 第 098 包。
  更新方式請參考：管理者介面更新操作手冊。

- **客製版：**
  確認系統版本，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：

```
mp701806301952    2020/06/30 14:41:21
mp701806301709    2020/06/30 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。