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-16-001**

**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 18 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 m2k_noc@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：**2016 / 2 / 17

**威脅類別：**CGI 修補

**威脅程度：**2 (分數 1~5，5 代表資安事件威脅程度很高)

**影響產品版本：**Mail2000 4.5/6.0/7.0

**事件摘要：**

CGI（Common Gateway Interface）是一個重要而且現在網站普遍應用的網路技術，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。Openfind 經資安團隊舉報，發現 Mail2000 4.5/6.0/7.0 有一 CGI 程式具備安全性問題，Openfind 已經在第一時間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此事。

**建議措施：**

- 建議所有使用 Mail2000 6.0/7.0 的客戶，立即更新安全性修正程式，以阻絕此潛在性風險。
- 建議所有使用 Mail2000 4.5 的客戶，因該版本維護期限已過，不再進行更新，請洽業務人員進行升級至最新版本的 Mail2000 或請與本公司技術人員洽詢，防止潛在安全性問題發生。

**更新方式：**

針對 Mail2000 6.0 或以上的客戶，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或可在 Openfind 的官方網頁下載安全性修正程式，自行進行更新。

- 標準版：

  Mail2000 6.0 客戶：

  請由線上更新頁面，依序更新 Patch 至 SP4 第 119 (160202) 包。


  Mail2000 7.0 客戶：

  請由線上更新頁面，依序更新 Patch 至 SP1 第 009 (160203) 包。

- 客製版：

  確認系統版本

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

```
mp601412221626  2015/01/06 14:41:21
mp601412261508  2015/01/06 14:41:51
```

  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。

**下載網址：**

OF-ISAC-16-001 安全性修正程式更新包：

http://www.openfind.com/taiwan/resource.html

**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。