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-17-006**

**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 19 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：**2017 / 6 / 13

**威脅類別：**CGI 漏洞

**威脅程度：**3 (分數 0~5，5 代表資安事件威脅程度很高)

**影響產品版本：** Mail2000 6.0 至 7.0 SP2 之間的版本

Openfind 發現 Mail2000 6.0 之後的版本，當透過正確的使用者帳號密碼登入後，在特定方法下能執行系統指令，產生安全性問題，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 至 7.0 SP2 的客戶，立即更新安全性修正程式，以阻絕此潛在性風險。
  ※ Mail2000 6.0 即將在 2017/6/30 停止維護，為了確保您系統的安全，請盡快升級至 7.0 版。
- 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：
  1. 密碼原則設定：管理者應透過此功能，強制規範全部使用者使用強度足夠的密碼、並定期更新、定期稽核。另可應用「圖形驗證」及「虛擬鍵盤」功能防止密碼被側錄。
  2. 登入使用 OTP (雙重認證)：系統管理者或持有敏感資料的帳號，登入時應要求使用雙重認證的方式，以確保只有帳號擁有者能登入存取。
  3. 限制登入 IP 或開啟異常登入警示：網域或帳號層級，可設定僅允許特定 IP 網段登入該帳號，甚至透過等級設定，限定各帳號能使用的收發信協定。另可設定「異常登入警示」功能，系統將自動監控除「境域白名單」或「IP 白名單」之外的登入行為，加以限制或自動通報。
  4. 使用 HTTPS、TLS 加密通道：電子郵件系統在 Webmail 或 SMTP、POP3 及 IMAP4 連線上，都應在主機端設定好 TLS 加密環境，並要求所有用戶修改設定強制以加密方式連線。

**更新方式：**

Mail2000 6.0 或以上的客戶，可透過兩種方式更新系統、修補漏洞： (1) 聯繫 Openfind 技術服務團隊，我們將協助您更新系統；(2) 您可使用產品線上更新功能，自行更新系統，相關版本資訊如下：

- 標準版：

  Mail2000 6.0 客戶：

  請由線上更新頁面，依序更新 Patch 至 SP4 第 134 包。

  ※ Mail2000 6.0 即將在 2017/6/30 停止維護，為了確保您系統的安全，請盡快升級至 7.0 版

  Mail2000 7.0 客戶：

  請由線上更新頁面，依序更新 Patch 至 SP2 第 036 包。

  ※ 若貴公司的版本為 7.0 至 7.0 SP1，請先洽詢 Openfind 技術客服預約升級服務


- 客製版：

  欲確認客製系統版本，請執行以下指令：

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

  輸出範例如下：

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

  請將紅字部分系統版號提供給網擎資訊，將提供安全性程式更新包。

**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。