

Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-19-003

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 / 03 / 21

威脅類別：CalDAV 與 RSS 漏洞修正

威脅程度：4 (分數 1~5，5 代表資安事件威脅程度很高)

影響產品版本：Mail2000 產品客戶

事件摘要：

- CalDAV

CalDAV 是一種用於存取網路行事曆、行程或會議排程的裝置與伺服器間之協定，經常用於手機與系統間之同步。Openfind 資安測試人員於例行測試中，發現相關程式安全性問題，已第一時間修正並主動提供安全性修正程式 (Security Patch)。

- RSS 服務

RSS (簡易資訊聚合) 是一種訊息來源格式規範，使用者可簡單訂閱如部落格文章、新聞等。由 RSS 「訂閱」的特性，當使用者主動訂閱電子新聞或部落格時，只要所訂閱的內容進行更新，該機制就會主動將更新內容送到使用者電腦中。此特性容易讓用戶因自動下載的功能而成為攻擊的標的。此次發現之漏洞須搭配較複雜之攻擊手法，並且發生在已於 2017 年停止維護之 V6 版本。若為 Mail2000 V7 版本之用戶則已無此使用者功能，此次亦重新檢視 V7 版本可能有影響之部分並提供安全性修正程式 (Security Patch)。

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 SP3 第 069 (190320) 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。