DEVCORE 剖析 Mail2000 漏洞已於去年修補正式聲明

有鑑於駭客攻擊手法日新月異，為展現 Openfind 在面對資安威脅的具體作為與回應能力，Openfind 主動與戴夫寇爾長期合作，提供測試環境以進行紅隊演練，日前由戴夫寇爾主辦的 DEVCORE Conference 2019 議程中提及的 CGI 漏洞即為去年初演練時發現，Openfind 研發團隊立即於修復後發佈資安通報 (OF-ISAC-18-002 及 OF-ISAC-18-003) 給產品客戶進行更新。

為提供客戶穩定、安全、可靠的郵件安全系統與服務，Openfind 郵件安全研究團隊長期主動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。網擎資訊執行長廖長健指出：「未來除了與戴夫寇爾持續合作進行紅隊演練外主動發掘系統問題外，也將持續參與各項有助於提昇資安等級的計畫，相信 Openfind 在 SSDLC 等軟體開發安全之投資與成果，絕對是超越客戶期待的。」

針對 DEVCORE 剖析 Mail2000 進階攻擊手法一事，引起媒體對於此事件的關切，並發出相關報導文章，導致客戶對於 Openfind 產品有安全上的疑慮及恐慌，我們為此深感抱歉。Openfind 將持續努力提升產品資安等級，也提醒客戶隨時留意資安通報及確認版本是否為最新版。

網擎資訊軟體股份有限公司謹啟

2019 年 10 月 16 日

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-19-007

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 / 10 / 16

威脅類別：CGI 漏洞

威脅程度：4.5（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：

此次資安通報為 2018 年 5 月 2 日已發佈之編號：OF-ISAC-18-002 之再度聲明，Openfind 已於 2018 年 5 月第一時間主動提供安全性修正程式（Security Patch）V7 SP3 第 050 (180417) 包與相關解決方法協助客戶處理完成，為了您系統的安全，Openfind 也建議您更新至目前的最新版本，詳情請參考下面建議措施之更新方式。

CGI（Common Gateway Interface）為現今網站普遍應用的重要網路技術，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。此一 CGI 漏洞須透過相當罕見的攻擊手法，利用極難發現的緩衝區溢位之途徑入侵；該手法有別於以往的攻擊方式，屬於相當進階且需要耗費大量時間才能計算出入侵點之攻擊手法，截至目前為止，尚未發現任何客戶單位實際遭此方式攻擊，因此尚未造成影響。

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 077 (190920) 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
```

```
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。