教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2021121603120000	發佈時間	2021-12-16 15:50:01
事故類型	ANA-漏洞預警	發現時間	2021-12-16 15:50:01
影響等級	中		

[主旨說明:][漏洞預警] Openfind 郵件安全威脅與潛在資安風險通報 (編號：OF-ISAC-21-001)

[內容說明:]

轉發 Openfind 郵件安全威脅與潛在資安風險通報(編號：OF-ISAC-21-001)

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。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

[影響平台:] Mail2000 7.0

[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	客製版
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。	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

[參考資料:]

1、https://cert.tanet.edu.tw/pdf/openfind20211216.pdf