張貼日期：2023/03/21

【資安漏洞預警】網擎資訊Mail2000電子郵件系統存在安全漏洞，請儘速確認並進行更新！

- 主旨說明：網擎資訊Mail2000電子郵件系統存在安全漏洞，允許攻擊者以XSS跨站腳本與複合式攻擊竊取使用者機敏資訊，請儘速確認並進行更新！

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202303-1085
  - 本院近期發現網擎資訊Mail2000電子郵件系統存在安全漏洞，允許攻擊者以XSS跨站腳本與複合式攻擊竊取使用者機敏資訊。攻擊者將前述漏洞之攻擊程式碼注入社交工程郵件，並寄發至受影響之Mail2000電子郵件系統，當使用者透過Webmail開啟社交工程郵件，將觸發XSS跨站腳本攻擊並連線至外部含惡意程式碼之網頁，導致使用者遭竊取個人機敏資訊，包含Cookie資訊、帳號身份相關資訊及電子郵件檔案等。
- 影響平台:
  - Mail2000 V7(含)以前版本
- 建議措施:
  1. 目前網擎資訊官方已針對此漏洞釋出程式更新公告，請各單位儘速聯繫Openfind 技術服務團隊或維護廠商，參考以下連結進行更新：https://www.openfind.com.tw/taiwan/resource.html
  2. 建議使用Mail2000電子郵件系統之單位，採用支援內容安全策略(Content Security Policies, CSP)之瀏覽器訪問Webmail以緩解XSS跨站腳本攻擊。
  3. 已知支援CSP之瀏覽器版本如下：
     - Chrome 59(含)版本以上
     - Edge 79(含)版本以上
     - Safari 15.4(含)版本以上
     - Firefox 58(含)版本以上
- 參考資料:
  1. https://www.openfind.com.tw/taiwan/resource.html
  2. https://openfind.freshdesk.com/support/solutions/articles/35000001733
  3. https://content-security-policy.com/
  4. Openfind 郵件安全威脅與潛在資安風險通報_OF-ISAC-23-002 https://www.openfind.com.tw/taiwan/download/Openfind_OF-ISAC-23-002.pdf

---

計算機與通訊中心
網路系統組 敬啟