張貼日期：2019/11/21

【資安漏洞預警】Openfind MAIL2000 Webmail Pre-Auth Cross-Site Scripting and Open Redirect

主旨：Openfind MAIL2000 Webmail Pre-Auth Cross-Site Scripting and Open Redirect

說明：

- 內容說明
  - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-ANA-201911-0002、TWCERTCC-ANA-201911-0003、TWCERTCC-ANA-201911-0004
  - TWCERTCC-ANA-201911-0002(CVE-2019-15071)：
    在MAIL2000 v 6.0 與 v7.0 之cgi-bin頁面下存在cross-site scripting (XSS)漏洞，在未授權的情況下可透過ACTION 參數執行惡意程式碼。
  - TWCERTCC-ANA-201911-0003(CVE-2019-15072)：
    在MAIL2000 v 6.0 與 v7.0 之cgi-bin 登入頁面下存在cross-site scripting (XSS)漏洞，在未授權的情況下可透過任何參數執行惡意程式碼。
    - 資安通報編號 OF-ISAC-19-003 (2019/03/21 發送)
    - Patch 069 修正 (2019/03/20 發佈)
  - TWCERTCC-ANA-201911-0004(CVE-2019-15073)：
    在MAIL2000 v 6.0 與 v7.0 存在Open Redirect之漏洞，在任何瀏覽器上開啟MAIL2000皆可在未授權的情況下轉址至惡意網站。
    - 資安通報編號 OF-ISAC-19-005 (2019/09/19 發送)
    - Patch 076 修正 (2019/09/17 發佈)
- 影響平台: MAIL2000 v 6.0 與 v7.0
- 建議措施:
  更新至最新版本
- 參考資料:
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15071
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15072
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15073

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20191121_01

Last update: **2019/11/22 15:09**