

張貼日期：2023/07/11

## 【資安訊息】請加強檢視各學校相關假冒FB帳號

- 主旨說明：轉教育部通知，本部發現近期有疑似偽冒學校名稱開立FB帳號，為大陸宣傳不利台灣之訊息，有明顯的政治操作意圖，請各單位加強自行檢查是否存在類似情況，避免遭受利用損及學校名譽等相關情事發生。
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202306-0439
  - 研究人員發現Barracuda ESG存在遠端命令注入(Remote Command Injection)漏洞(CVE-2023-2868)該漏洞源自於對使用者提供的.tar檔案未有適當之輸入驗證(Improper input validation)該漏洞在去(2022)年10月已遭駭客利用，攻擊者可於未經身分鑑別之情況下，藉由寄送偽造附件之電子郵件觸發此漏洞，進而遠端執行任意程式碼。
- 影響平台：
  - Facebook等社群平台
- 建議措施：
  1. 檢視Facebook等社群平台有無假冒帳號。
  2. 檢舉假冒Facebook 帳號或粉絲專頁  
[https://zh-tw.facebook.com/help/174210519303259/?helpref=related\\_articles](https://zh-tw.facebook.com/help/174210519303259/?helpref=related_articles)
- 參考資料: 無

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/mailling:announcement:20230711\\_01](https://net.nthu.edu.tw/netsys/mailling:announcement:20230711_01)

Last update: **2023/07/11 14:05**

