**張貼日期：2023/06/30**

# 【資安漏洞預警Barracuda電子郵件安全閘道器(Email Security GatewayESG)存在高風險安全漏洞(CVE-2023-2868)請儘速確認並進行更新或評估採取緩解措施。

- 主旨說明Barracuda電子郵件安全閘道器(Email Security GatewayESG)存在高風險安全漏洞(CVE-2023-2868)允許攻擊者於未經身分鑑別之情況下，遠端執行任意程式碼，該漏洞目前已遭駭客利用，請儘速確認並進行更新或評估採取緩解措施。
- 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)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:
  - Barracuda ESG(僅限實體設備)5.1.3.001至9.2.0.006版本
- 建議措施:
  - Barracuda原廠表示，已於5/21透過強制更新機制，套用2個針對此漏洞之修補程式自動完成修補。雖然漏洞已經自動修補完成，但採用Barracuda ESG產品之系統管理者仍應檢視其應用環境是否有遭到駭侵攻擊得逞之跡象。若已遭駭侵，則建議立即更新設備以策安全。
- 參考資料:
  1. https://www.barracuda.com/company/legal/esg-vulnerability
  2. https://nvd.nist.gov/vuln/detail/CVE-2023-2868
  3. https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

---

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:20230630_01**

Last update: **2023/06/30 08:53**