張貼日期：2024/04/17

【漏洞預警Palo Alto Networks PAN-OS存在高風險安全漏洞(CVE-2024-3400)請儘速確認並進行修補！

- 主旨說明Palo Alto Networks PAN-OS存在高風險安全漏洞(CVE-2024-3400)請儘速確認並進行修補！
- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202404-00000076
  - 研究人員發現Palo Alto Networks PAN-OS存在作業系統命令注入(OS Command Injection)漏洞(CVE-2024-3400)未經身分鑑別之遠端攻擊者，可利用此漏洞於防火牆以最高權限(root)執行任意程式碼。該漏洞目前已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
  - PAN-OS 10.2.9-h1(不含)以前版本
  - PAN-OS 11.0.4-h1(不含)以前版本
  - PAN-OS 11.1.2-h3(不含)以前版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請更新至以下版本：
    - PAN-OS 10.2系列請更新至10.2.9-h1(含)以後版本
    - PAN-OS 11.0系列請更新至11.0.4-h1(含)以後版本
    - PAN-OS 11.1系列請更新至11.1.2-h3(含)以後版本
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2024-3400
  2. https://security.paloaltonetworks.com/CVE-2024-3400

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:20240417_01

Last update: **2024/04/17 09:41**