張貼日期：2020/09/17

【資安漏洞預警PAN-OS之Captive Portal或多因素驗證(Multi-Factor Authentication, MFA)介面存在安全漏洞，請儘速確認並進行更新

主旨：【資安漏洞預警PAN-OS之Captive Portal或多因素驗證(Multi-Factor Authentication, MFA)介面存在安全漏洞(CVE-2020-2040)允許攻擊者以root權限執行任意程式碼，請儘速確認並進行更新

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NISAC-ANA-202009-0552
  - PAN-OS為運行於Palo Alto Networks新世代防火牆之作業系統，研究人員發現PAN-OS之Captive Portal或多因素驗證(Multi-Factor Authentication, MFA)介面存在緩衝區溢位漏洞(CVE-2020-2040)未經身分驗證的攻擊者可藉由發送惡意請求，利用此漏洞進而以root權限執行任意程式碼。
- 影響平台:
  受影響PAN-OS版本如下:
  - PAN-OS 9.1PAN-OS 9.1.3以前版本
  - PAN-OS 9.0PAN-OS 9.0.9以前版本
  - PAN-OS 8.1PAN-OS 8.1.15以前版本
  - PAN-OS 8.0所有版本
- 建議措施:
  目前Palo Alto Networks官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考以下建議進行更新：
  1. 請登入設備並檢視Dashboard資訊，或於指令介面輸入show system info指令，確認當前使用之PAN-OS版本，並於Web介面中確認是否啟用Captive Portal或多因素驗證功能。
  2. 如使用受影響之PAN-OS版本，且啟用Captive Portal或多因素驗證功能，請瀏覽官方公告網頁(https://security.paloaltonetworks.com/CVE-2020-2040)進行PAN-OS版本更新。
- 參考資料:
  1. https://securitypaloaltonetworks.com/CVE-2020-2040
  2. https://nvd.nist.gov/vuln/detail/CVE-2020-2040
  3. https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/authentication/configure-multi-factor-authentication.html

---

計算機與通訊中心
網路系統組 敬啟