張貼日期：2020/07/01

【資安漏洞預警PAN-OS之SAML身分驗證功能存在安全漏洞(CVE-2020-2021)允許攻擊者存取受保護之資料，或以管理員身分登入設備並執行管理操作，請儘速確認並進行更新

主旨：【資安漏洞預警PAN-OS之SAML身分驗證功能存在安全漏洞(CVE-2020-2021)允許攻擊者存取受保護之資料，或以管理員身分登入設備並執行管理操作，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-202007-0029
  - 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SAML功能存在身分驗證繞過漏洞(CVE-2020-2021)攻擊者可針對已啟用SAML身分驗證功能但並未勾選「驗證身分提供者憑證」選項之設備，利用此漏洞存取受保護之資料，或以管理員身分登入設備並執行管理操作。
- 影響平台:
  - PAN-OS 9.1PAN-OS 9.13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SAML身分驗證功能，以及是否勾選「驗證身分提供者憑證」選項。
  2. 如使用受影響之PAN-OS版本，且啟用SAML身分驗證功能但並未勾選「驗證身分提供者憑證」選項，請瀏覽官方公告網頁
- 參考資料:
  1. https://security.paloaltonetworks.com/CVE-2020-2021
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2021
  3. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-cli-quick-start/use-the-cli/view-settings-and-statistics.html
  4. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/configure-saml-authentication.html
  5. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-server-profiles-saml-identity-provider.html
  6. https://docspaloaltonetworks.com/content/dam/techdocs/zh_TW/pdf/pan-os/9-0/pan-os-90-admin-guide-zh-tw.pdf

---

計算機與通訊中心
網路系統組 敬啟