行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2020-0067	發布時間	Tue Jun 30 18:45:40 CST 2020
事件類型	漏洞預警	發現時間	Tue Jun 30 00:00:00 CST 2020
警訊名稱	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	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	受影響 PAN-OS 版本如下: PAN-OS 9.1：PAN-OS 9.1.3 以前版本 PAN-OS 9.0：PAN-OS 9.0.9 以前版本 PAN-OS 8.1：PAN-OS 8.1.15 以前版本 PAN-OS 8.0：所有版本		
影響等級	高		
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(https://security.paloaltonetworks.com/CVE-2020-2021)進行 PAN-OS 版本更新。		

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://docs.paloaltonetworks.com/content/dam/techdocs/zh_TW/pdf/pan-os/9-0/pan-os-90-admin-guide-zh-tw.pdf

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw