

ANA事件單通知:TACERT-ANA-2026050605050101 【漏洞預警】 Palo Alto Networks PAN-OS存在重大資安漏洞(CVE-2026-0300)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026050605050101	發佈時間	2026-05-06 17:23:02
事故類型	ANA-漏洞預警	發現時間	2026-05-06 17:23:02
影響等級	低		

[主旨說明:] 【漏洞預警】 Palo Alto Networks PAN-OS存在重大資安漏洞(CVE-2026-0300)

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202605-00000002

Palo Alto Networks 的防火牆作業系統 PAN-OS的User-ID驗證入口網站服務存在緩衝區溢位漏洞(CVE-2026-0300, CVSS : 9.3), 此漏洞允許未經身分驗證的攻擊者透過發送特製的資料, 在PA系列和VM系統防火牆上, 以root權限執行任意程式碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」, 煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

PAN-OS 12.1.4-h5(不含)以前版本

PAN-OS 12.1.7(不含)以前版本

PAN-OS 11.2.4-h17(不含)以前版本

PAN-OS 11.2.7-h13(不含)以前版本

PAN-OS 11.2.10-h6(不含)以前版本

PAN-OS 11.2.12(不含)以前版本

PAN-OS 11.1.4-h33(不含)以前版本

PAN-OS 11.1.6-h32(不含)以前版本

PAN-OS 11.1.7-h6(不含)以前版本

PAN-OS 11.1.10-h25(不含)以前版本

PAN-OS 11.1.13-h5(不含)以前版本

PAN-OS 11.1.15(不含)以前版本

PAN-OS 10.2.7-h34(不含)以前版本

PAN-OS 10.2.10-h36(不含)以前版本

PAN-OS 10.2.13-h21(不含)以前版本

PAN-OS 10.2.16-h7(不含)以前版本

PAN-OS 10.2.18-h6(不含)以前版本

[建議措施:]

根據官方網站釋出的解決方式進行修補：<https://security.paloaltonetworks.com/CVE-2026-0300>

[參考資料:]

1. <https://www.twcert.org.tw/tw/cp-169-10898-012f2-1.html>

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw