

FW: 【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 !

1 封郵件

gz710@mail.ncku.edu.tw <gz710@mail.ncku.edu.tw>
收件者: nckucc_黃國展 <gz710@mail.ncku.edu.tw>
副本: nckucc_朱敏清 <kkinglord@mail.ncku.edu.tw>

2024年4月17日 上午8:09

各位老師好：

轉寄教育機構ANA通報平台通知 · 謝謝。

成大計網中心 敬上

連絡電話：06-2757575轉61037

From: service <service@cert.tanet.edu.tw>

Sent: Tuesday, April 16, 2024 4:49 PM

To: service@cert.tanet.edu.tw

Subject: (ANA事件單通知:TACERT-ANA-2024041604040505)(【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 !)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2024041604040505	發佈時間	2024-04-16 16:38:08
事故類型	ANA-漏洞預警	發現時間	2024-04-16 16:38:08
影響等級	中		
[主旨說明:] 【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 !			
[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。 情資分享等級: WHITE(情資內容為可公開揭露之資訊)			
[影響平台:] <ul style="list-style-type: none">● 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： <ul style="list-style-type: none">● 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:] <ol style="list-style-type: none">1. https://nvd.nist.gov/vuln/detail/CVE-2024-34002. https://security.paloaltonetworks.com/CVE-2024-3400			

(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