

**FW: 【漏洞預警】Zyxel 近日發布 防火牆與無線基地臺的安全性更新，建議請管理者儘速評估更新！**

1 封郵件

gz710@mail.ncku.edu.tw <gz710@mail.ncku.edu.tw>

2024年3月5日 上午9:21

收件者: nckucc\_黃國展 <gz710@mail.ncku.edu.tw>

副本: nckucc\_朱敏清 <kkinglord@mail.ncku.edu.tw>

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, March 5, 2024 9:19 AM

To: service@cert.tanet.edu.tw

Subject: (ANA事件單通知:TACERT-ANA-2024030508031818)(【漏洞預警】Zyxel 近日發布 防火牆與無線基地臺的安全性更新，建議請管理者儘速評估更新！)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2024030508031818	發佈時間	2024-03-05 08:32:18
事故類型	ANA-漏洞預警	發現時間	2024-03-05 08:32:18
影響等級	中		
[主旨說明:]【漏洞預警】Zyxel 近日發布 防火牆與無線基地臺的安全性更新，建議請管理者儘速評估更新！			
[內容說明:] 轉發 中華資安國際 CHTSECURITY-200-202403-00000001  ● CVE-2023-6397 某些防火牆版本存在空指標解引用漏洞，如果防火牆啟用了「反惡意軟體」功能，則允許基於區域網路 (LAN) 的攻擊者，透過經過特別製作的RAR壓縮文件，下載到LAN端主機，進而引起服務阻斷 (DoS) 條件。  ● CVE-2023-6398 在某些防火牆和存取點 (AP) 版本中，文件上傳二進制檔的繞過身份驗證命令注入漏洞，經過身份驗證的攻擊者可能具有管理員權限，透過FTP在受影響的設備上執行一些操作系統 (OS) 命令。  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」，煩請貴單位協助公告或轉發			
[影響平台:] ● 防火牆 ● 無線基地臺			
[建議措施:] 請參考 Zyxel 官方網站的說明和處理建議更新版本： <a href="https://www.zyxel.com/tw/zh/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-aps-02-21-2024">https://www.zyxel.com/tw/zh/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-aps-02-21-2024</a>			
[參考資料:]			

(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](mailto:service@cert.tanet.edu.tw)