張貼日期：2023/05/04

【資安漏洞預警Zyxel防火牆存在安全漏洞CVE-2023-27991與CVE-2023-28771允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

- 主旨說明Zyxel防火牆存在安全漏洞CVE-2023-27991與CVE-2023-28771允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202305-0115
  - 研究人員發現Zyxel防火牆存在2個高風險安全漏洞 CVE-2023-27991為命令注入漏洞，允許已通過身分鑑別之遠端攻擊者，透過命令列介面，執行作業系統指令，達到任意執行程式碼情況 CVE-2023-28771為命令注入漏洞，允許未經身分鑑別之遠端攻擊者，透過發送偽造網路封包，執行作業系統指令，達到任意執行程式碼情況。
- 影響平台：
  1. CVE-2023-27991
     1. ATP系列產品之韌體版本ZLD V4.32至V5.35
     2. USG-FLEX系列產品之韌體版本ZLD V4.50至V5.35
     3. USG FLEX 50(W)/USG20(W)-VPN系列產品之韌體版本 ZLD V4.16至V5.35
     4. VPN系列產品之韌體版本ZLD V4.30至V5.35
  2. CVE-2023-28771
     1. ATP系列產品之韌體版本ZLD V4.60至V5.35
     2. USG-FLEX系列產品之韌體版本ZLD V4.60至V5.35
     3. VPN系列產品之韌體版本ZLD V4.60至V5.35
     4. ZyWALL/USG系列產品之韌體版本ZLD V4.60至V4.73
- 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：
    1. ATPUSG-FLEXUSG FLEX 50(W)USG20(W)-VPN及VPN等系列產品之韌體版本請更新至ZLD V5.36(含)以上版本。
    2. ZyWALL/USG系列產品之韌體版本請更新至ZLD V4.73 Patch 1(含)以上版本。
- 參考資料：
  1. https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls
  2. https://nvd.nist.gov/vuln/detail/CVE-2023-27991
  3. https://nvd.nist.gov/vuln/detail/CVE-2023-28771
  4. https://thehackernews.com/2023/04/zyxel-firewall-devices-vulnerable-to.html

—- 計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20230504_01

Last update: **2023/05/05 09:42**