張貼日期：2024/10/07

【漏洞預警】普萊德科技交換器設備存在多個高風險漏洞

- 主旨說明：SonicOS存在高風險安全漏洞(CVE-2024-40766)，請儘速確認並進行修補
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202410-00000001：
  - 【普萊德科技交換器設備 - Remote privilege escalation using hard-coded credentials】(CVE-2024-8448，CVSS 3.x：8.8) 普萊德科技部分交換器型號之特定命令列介面存在hard-coded帳號通行碼，已取得一般權限之遠端攻擊者以該組帳密登入後可取得Linux root shell.
  - 【普萊德科技交換器設備 - Missing Authentication for multiple HTTP routes】(CVE-2024-8456，CVSS 3.x：9.8) 普萊德科技部分交換器型號之韌體上傳與下載功能缺乏適當的存取控制，允許未經身分鑑別的遠程攻擊者下載與上傳韌體、系統組態設定，最終獲得設備的完全控制權。
  - 【普萊德科技交換器設備 - Cross-site Request Forgery】 (CVE-2024-8458，CVSS 3.x：8.8) 普萊德科技部分交換器型號之網頁應用程式存在Cross-Site Request Forgery(CSRF)漏洞，未經身分鑑別之遠端攻擊者誘騙使用者瀏覽惡意網站後，可假冒該使用者身分進行操作，例如新增帳號。
- 影響平台:
  - GS-4210-24PL4C hardware 2.0
  - GS-4210-24P2S hardware 3.0
- 建議措施:
  1. 更新 GS-4210-24PL4C hardware 2.0 之韌體至 2.305b240719(含)以後版本。
  2. 更新 GS-4210-24P2S hardware 3.0 之韌體至 3.305b240802(含)以後版本。
- 參考資料:
  1. 普萊德科技交換器設備 - Remote privilege escalation using hard-coded credentials：https://www.twcert.org.tw/tw/cp-132-8045-a2804-1.html
  2. 普萊德科技交換器設備 - Missing Authentication for multiple HTTP routes：https://www.twcert.org.tw/tw/cp-132-8061-91872-1.html
  3. 普萊德科技交換器設備 - Cross-site Request Forgery：https://www.twcert.org.tw/tw/cp-132-8065-579c1-1.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:20241007_01

Last update: **2024/10/07 09:30**