張貼日期：2025/02/25

【漏洞預警】SonicWall SonicOS存在安全漏洞(CVE-2024-53704)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】SonicWall SonicOS存在安全漏洞(CVE-2024-53704)，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-200-202502-00000128，
  - 研究人員發現SonicWall SonicOS存在不當驗證(Improper Authentication)漏洞(CVE-2024-53704)，允許未經身分鑑別之遠端攻擊者劫持任意SSLVPN連線，進而滲透內部私人網路。該漏洞利用方式已公開，請儘速確認並進行修補。
- 影響平台:
  - Gen7 Firewalls 7.1.1-7058(含)以前版本與7.1.2-7019版本
  - Gen7 NSv 7.1.1-7058(含)以前版本與7.1.2-7019版本
  - TZ80 8.0.0-8035版本
- 建議措施:
  - 受影響之產品以及其韌體版本如下 Gen7 Firewalls：TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 7.1.1-7058(含)以前版本與7.1.2-7019版本 Gen7 NSv：NSv 270, NSv 470, NSv 870 7.1.1-7058(含)以前版本與7.1.2-7019版本 TZ80 8.0.0-8035版本
  - 官方已針對漏洞釋出修復更新，請參考官方說明，網址如下：https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003
- 參考資料:
  1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003
  2. https://nvd.nist.gov/vuln/detail/CVE-2024-53704
  3. https://www.zerodayinitiative.com/advisories/ZDI-25-012/
  4. https://bishopfox.com/blog/sonicwall-cve-2024-53704-ssl-vpn-session-hijacking

---

計算機與通訊中心
網路系統組 敬啟