張貼日期：2025/08/04

【漏洞預警】Sophos 的防火牆系統存在3個重大資安漏洞

- 主旨說明:【漏洞預警】Sophos 的防火牆系統存在3個重大資安漏洞

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202507-00000021
  - Sophos發布關於防火牆的資安公告，指出旗下的防火牆產品存在3個重大資安漏洞，並提出修補版本，呼籲用戶儘快檢查系統是否套用相關更新。
  - 【CVE-2025-6704】(CVSS：9.8) 安全PDF交換(Secure PDF eXchange，SPX)功能存在任意文件寫入漏洞，若啟用SPX的特定配置且防火牆處於高可用性(HA)模式，可能導致預授權遠端程式碼執行。
  - 【CVE-2025-7624】(CVSS：9.8) Legacy (transparent) SMTP proxy存在一項SQL注入漏洞，若電子郵件啟用隔離政策，且系統從21.0 GA之前的版本升級至現有版本，可能導致遠端程式碼執行。
  - 【CVE-2025-7382】(CVSS：8.8) WebAdmin 存在命令注入漏洞，若管理員啟用OTP驗證，則可能導致相鄰攻擊者在高可用性(HA)輔助設備上實現預授權程式碼執行。
- 影響平台:
  - Sophos Firewall v21.5 GA (含)以前版本
- 建議措施:
  - 根據官方網站釋出解決方式進行修補：
    https://www.sophos.com/en-us/security-advisories/sophos-sa-20250721-sfos-rce
- 參考資料:
  - https://www.twcert.org.tw/tw/cp-169-10280-e36be-1.html

計算機與通訊中心
網路系統組 敬啟