張貼日期：2026/07/22

【漏洞預警SonicWall SMA 1000系列存在多項高風險安全漏洞(CVE-2026-15409與CVE-2026-15410)請儘速確認並進行修補

- 主旨說明:【漏洞預警SonicWall SMA 1000系列存在多項高風險安全漏洞(CVE-2026-15409與CVE-2026-15410)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 資安訊息警訊 NISAC-200-202607-00000005
  - 研究人員發現SonicWall SMA 1000系列存在多項高風險安全漏洞(CVE-2026-15409與CVE-2026-15410)類型分別為伺服器端請求偽造(Server-Side Request Forgery)與程式碼注入(Code Injection)兩項漏洞皆已遭到駭客利用，請儘速確認並進行修補 CVE-2026-15409未經身分鑑別之遠端攻擊者可對SMA1000設備之Work Place介面發送特製請求，進而使系統向非預期位置發送請求 CVE-2026-15410已取得管理員權限之遠端攻擊者可於Appliance Management Console(AMC)執行任意作業系統指令。
- 影響平台:
  - SonicWall SMA 1000系列(6210、7210及8200v)
  - platform-hotfix 12.4.3-03245~12.4.3-03387及12.4.3-03434版本
  - platform-hotfix 12.5.0-02283~12.5.0-02624及12.5.0-02800版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請升級至以下版本，並參考官方說明進行更新：https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-15409
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-15410
  3. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
  4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

---

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:20260722_21

Last update: **2026/07/22 10:28**