**張貼日期：2026/09/10**

# 【漏洞預警】SonicWall NSM On-Prem與SMA1000系列存在多項高風險安全漏洞(CVE-2026-78327、CVE-2026-83548及CVE-2026-83549)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】SonicWall NSM On-Prem與SMA1000系列存在多項高風險安全漏洞(CVE-2026-78327、CVE-2026-83548及CVE-2026-83549)，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-200-202609-00000008
  - 研究人員發現SonicWall NSM On-Prem與SMA1000系列存在多項高風險安全漏洞(CVE-2026-78327、CVE-2026-83548及CVE-2026-83549)，類型包含作業系統指令注入(OS Command Injection)與伺服器請求偽造(Server-Side Request Forgery)，其中CVE-2026-83548與CVE-2026-83549已遭駭客利用，請儘速確認並進行修補。
  - CVE-2026-78327 已取得管理權限之遠端攻擊者，可藉由於管理介面注入任意作業系統指令，進而於底層主機執行任意程式碼。
  - CVE-2026-83548 未經身分鑑別之遠端攻擊者可利用非預期之替代存取路徑，存取敏感功能並執行未經授權之操作。
  - CVE-2026-83549 於特定條件下，已通過身分鑑別之遠端攻擊者，可透過管理主控台(AMC)以管理員身分執行任意作業系統指令，進而執行任意程式碼。
- 影響平台:
  - SonicWall NSM On-Prem(VMware、Hyper-V、Azure及KVM)之4.3.0(含)以前版本
  - SonicWall SMA1000系列(6210、7210及8200v) platform-hotfix 12.4.3-03453(含)以前版本
  - SonicWall SMA1000系列(6210、7210及8200v) platform-hotfix 12.5.0-02835(含)以前版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：
  1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0015
  2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-78327
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-83548
  3. https://nvd.nist.gov/vuln/detail/CVE-2026-83549

---

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:20260910_24**

Last update: **2026/09/10 16:28**