教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026090908090808	發佈時間	2026-09-09 08:36:09
事故類型	ANA-漏洞預警	發現時間	2026-09-09 08:36:09
影響等級	中		

[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。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[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