張貼日期：2021/09/28

【資安漏洞預警□SonicWall之SMA 100系列SSL VPN設備存在安全漏洞(CVE-2021-20034)□請儘速確認並進行更新！

- 主旨說明：【資安漏洞預警□SonicWall之SMA 100系列SSL VPN設備存在安全漏洞(CVE-2021-20034)□允許攻擊者繞過目錄遍歷檢查並刪除任意檔案，請儘速確認並進行更新！

- 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-ANA-202109-1472□
  - 研究人員發現SonicWall之SMA 100系列SSL VPN設備存在安全漏洞(CVE-2021-20034)□肇因於存取控制失當，導致攻擊者可繞過目錄遍歷檢查並刪除任意檔案，進而造成設備重新啟動並還原至出廠設定。
- 影響平台:
  - SMA 100系列(SMA 200□SMA 210□SMA 400□SMA 410及SMA 500v (ESX, KVM, AWS, Azure))之以下版本：
    - 10.2.1.0-17sv(含)以前版本
    - 10.2.0.7-34sv(含)以前版本
    - 9.0.0.10-28sv(含)以前版本
- 建議措施:
  - 目前SonicWall官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商參考下方步驟進行版本更新：https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-del
- 參考資料:
  1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0021
  2. https://thehackernews.com/2021/09/sonicwall-issues-patches-for-new.html
  3. https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-delete-vulnerability-in-sonicwall-sma-100-series-appliances/210819124854603/

計算機與通訊中心
網路系統組 敬啟