張貼日期：2021/02/08

【資安漏洞預警□SonicWall之SMA 100系列SSL VPN設備存在安全漏洞(CVE-2021-20016)□允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

主旨：【資安漏洞預警□SonicWall之SMA 100系列SSL VPN設備存在安全漏洞(CVE-2021-20016)□允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NISAC-ANA-202102-0283
  - 研究人員發現SonicWall之SMA 100系列SSL VPN設備存在SQL注入漏洞(CVE-2021-20016)□攻擊者可利用該漏洞取得帳密資訊，進而獲得管理員權限，並可遠端執行任意程式碼。
- 影響平台:
  使用10.x韌體版本之SMA 100系列SSL VPN設備如下：
  - 實體設備□SMA 200□SMA 210□SMA 400及SMA 410
  - 虛擬設備□SMA 500v
- 建議措施:
  - 目前SonicWall官方已針對此漏洞釋出更新程式(https://wwwsonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/)，請各機關聯絡設備維護廠商參考下方步驟進行版本更新：
    1. 將設備更新至10.2.0.5-29sv版本，並重置設備上所有帳號之密碼，以及啟用多因素驗證(Multi-Factor Authentication, MFA)功能。
    2. 若無法立即更新，可啟用WAF功能進行緩解，參考連結：https://www.sonicwall.com/support/knowledge-base/how-to-configure-web-application-fir
- 參考資料:
  1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001
  2. https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20016
  4. https://www.sonicwall.com/support/knowledge-base/how-to-configure-web-application-firewall-waf-on-the-sma-100-series/210202202221923/
  5. https://www.sonicwall.com/support/knowledge-base/how-to-upgrade-firmware-on-sma-100-series-appliances/170502339501169/
  6. https://www.sonicwall.com/support/knowledge-base/smb-ssl-vpn-upgrading-firmware-on-sma-500v-virtual-appliance/170502851052498/
  7. https://www.sonicwall.com/support/knowledge-base/how-can-i-check-the-current-firmware-version-of-your-sonicwall/170504764898494/

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:20210208_02

Last update: **2021/02/08 13:58**