張貼日期：2022/04/06

【資安漏洞預警SonicWall SonicOS存在安全漏洞(CVE-2022-22274)請儘速確認並進行更新!

- 主旨說明SonicWall SonicOS存在安全漏洞(CVE-2022-22274)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 國家資安資訊分享與分析中心 NISAC-ANA-202204-0007
  - SonicOS是SonicWall防火牆所使用之作業系統，研究人員發現SonicOS存在堆疊記憶體緩衝溢位(Stack-based buffer overflow)漏洞，遠端攻擊者可藉由發送特製之HTTP請求，利用此漏洞進行阻斷服務攻擊或執行任意程式碼。
- 影響平台：
  1. SonicWall FireWalls
     1. 型號TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 870
     2. SonicOS版本：7.0.1-5050(含)以前版本
  2. SonicWall NSsp Firewall
     1. 型號NSsp 15700
     2. SonicOS版本7.0.1-R579(含)以前版本
  3. SonicWall NSv Firewalls
     1. 型號NSv 10, NSv 25, NSv 50, Nsv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600
     2. SonicOS版本6.5.4.4-44v-21-1452(含)以前版本
- 建議措施：
  1. 目前SonicWall官方已針對此漏洞釋出部份更新程式，請各機關可聯絡設備維護廠商進行下列版本更新作業：
     1. SonicWall FireWalls請更新至7.0.1-5051(含)以上版本。
     2. SonicWall NSsp Firewall請採取緩解措施，僅允許受信任之來源IP可連線至管理介面，或安裝7.0.1-5030-HF-R844修補程式。俟SonicWall官方4月中釋出新版程式後，再進行SonicOS升版作業。
     3. SonicWall NSv Firewalls請更新至6.5.4.4-44v-21-1519(含)以上版本。
  2. 設備管理者登入管理介面後，可於監控功能頁面之系統狀態資訊中，得知該設備所使用之SonicOS版本。
- 參考資料：
  1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003
  2. https://nvd.nist.gov/vuln/detail/CVE-2022-22274
  3. https://www.bleepingcomputer.com/news/security/critical-sonicwall-firewall-patch-not-released-for-all-devices/

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:20220406_01

Last update: **2022/04/06 09:47**