張貼日期：2024/09/12

【漏洞預警】SonicOS存在高風險安全漏洞(CVE-2024-40766)，請儘速確認並進行修補

- 主旨說明：SonicOS存在高風險安全漏洞(CVE-2024-40766)，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 NISAC-200-202409-00000015，
  - 研究人員發現SonicOS存在不當存取控制(Improper Access Control)漏洞(CVE-2024-40766)，允許未經授權資源存取或於特定條件下導致防火牆失效，該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
  - SonicWall Firewall Gen 5: SonicOS 5.9.2.14-12o(含)以下版本
  - SonicWall Firewall Gen 6: SonicOS 6.5.4.14-109n(含)以下版本
  - SonicWall Firewall Gen 7: SonicOS 7.0.1-5035(含)以下版本
- 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：

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2024-40766
  2. https://www.cve.org/CVERecord?id=CVE-2024-40766
  3. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

計算機與通訊中心
網路系統組 敬啟