張貼日期：2022/03/29

【資安漏洞預警】Sophos Firewall作業系統存在安全漏洞(CVE-2022-1040)，請儘速確認並進行更新

- 主旨說明：Sophos Firewall作業系統存在安全漏洞(CVE-2022-1040)，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-202203-0951，
  - 研究人員發現Sophos Firewall作業系統之使用者入口(User portal)與網頁管理介面(Webadmin)存在身分驗證繞過漏洞(CVE-2022-1040)，導致攻擊者得以利用該漏洞繞過系統管控，以管理者權限執行任意程式碼。
- 影響平台:
  Sophos Firewall 18.5 MR3(含)以前版本
- 建議措施:
  1. 目前Sophos官方已針對此漏洞釋出更新程式，請各機關可聯絡設備維護廠商進行版本更新，並確認更新至18.5 MR4(含)或19.0 GA以上版本。
  2. 如欲沿用舊版本，可登入網頁管理介面並啟用「允許自動安裝修補程式(Allow automatic installation of hotfixes)」功能，設備將每隔30分鐘檢查一次並自動安裝新修補程式，即可完成安裝此漏洞之修補程式。
  3. 若未能及時修補漏洞，可使用VPN或Sophos Central進行遠端連線與管理，以確保Sophos Firewall之網頁管理介面不暴露於廣域網路(WAN)中，以提升遠端存取安全性。
- 參考資料:
  1. https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce
  2. https://nvd.nist.gov/vuln/detail/CVE-2022-1040
  3. https://www.bleepingcomputer.com/news/security/critical-sophos-firewall-vulnerability-allows-remote-code-execution/

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:20220329_01

Last update: **2022/03/30 07:41**