張貼日期：2020/05/05

【資安漏洞預警Sophos XG Firewall存在安全漏洞(CVE-2020-12271)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Sophos XG Firewall存在安全漏洞(CVE-2020-12271)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 資安訊息警訊 NISAC-ANA-202005-0030
  - 研究人員發現Sophos XG Firewall使用的SFOS存在資料庫注入(SQL injection)的安全漏洞(CVE-2020-12271)遠端攻擊者可對目標系統發送特製請求，利用此漏洞取得機敏資訊，進而執行任意程式碼。
- 影響平台:
  - XG Firewall中SFOS的所有版本皆受此漏洞影響：
    15.0 15.01
    16.01
    16.01.2
    16.01.3
    16.05.0
    16.05.1
    16.05.2
    16.05.3
    16.05.4
    16.05.5
    16.05.6
    16.05.7
    16.05.8
    17.0.0
    17.0.1
    17.0.2
    17.0.3
    17.1
    17.5
    18.0
- 建議措施:
  1. 目前Sophos官方已針對此漏洞釋出更新程式(僅17.0、17.1、17.5及18.0可收到自動更新)，請各機關聯絡設備維護廠商進行版本確認並更新，或依官方說明，開啟自動更新功能進行更新。
     - 官方公告連結如下：https://community.sophos.com/kb/en-us/135412
     - 開啟自動更新功能，請參考：https://community.sophos.com/kb/en-us/135415
  2. 其餘版本建議評估更新至提供修補更新程式之版本，如果無法更新，建議關閉管理介面(或對外之登入頁面服務)，或限制來源IP存取必要之對外服務。
- 參考資料:
  1. https://community.sophos.com/kb/en-us/135412
  2. https://news.sophos.com/en-us/2020/04/26/asnarok
  3. https://www.ithome.com.tw/news/137239

4. https://www.cybersecurity-help.cz/vdb/SB2020042601

計算機與通訊中心
網路系統組 敬啟