張貼日期：2022/10/24

【資安漏洞預警Sophos XG Firewall作業系統存在安全漏洞(CVE-2020-15504)允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

- 主旨說明Sophos XG Firewall作業系統存在安全漏洞(CVE-2020-15504)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-202210-0946
  - 研究人員發現Sophos XG Firewall作業系統之使用者入口(User Portal)與網頁管理介面(Webadmin)存在SQL注入漏洞(CVE-2020-15504)導致遠端攻擊者可執行任意程式碼。
- 影響平台：
  - Sophos XG Firewall v18.0 MR1版本(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v17.5 MR13與v18 MR-1-Build396(含)以上版本，若為更舊之版本則需更新到前述支援之版本再安裝修補程式。
  2. 另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。
- 參考資料：
  1. https://community.sophos.com/b/security-blog/posts/advisory-resolved-rce-via-sqli-cve-2020-15504
  2. https://www.sophos.com/en-us/security-advisories/sophos-sa-20200710-xg-sqli-rce
  3. https://nvd.nist.gov/vuln/detail/CVE-2020-15504
  4. https://www.tenable.com/cve/CVE-2020-15504

計算機與通訊中心
網路系統組 敬啟