張貼日期：2020/12/18

【資安漏洞預警SolarWinds Orion Platform部分版本存在後門程式，允許攻擊者遠端執行任意程式碼，請儘速確認並進行版本更新

主旨：【資安漏洞預警SolarWinds Orion Platform部分版本存在後門程式，允許攻擊者遠端執行任意程式碼，請儘速確認並進行版本更新

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NISAC-ANA-202012-0765
  - Orion Platform為SolarWinds所推出之整合式網路管理工具，具備功能模組化與擴展性特色FireEye研究人員發現其部分版本存在後門程式，並藉由更新機制進行散播，使得攻擊者可遠端操控系統並執行任意程式碼，進而利用運行於SolarWinds Orion Platform上之相關功能模組進行內部擴散，加劇危害程度。
- 影響平台:
  - SolarWinds Orion Platform 2019.4 HF 5
  - SolarWinds Orion Platform 2020.2
  - SolarWinds Orion Platform 2020.2 HF 1
- 建議措施:
  1. 目前SolarWinds官方已釋出更新程式，請各機關聯絡設備維護廠商進行版本確認，並瀏覽官方公告網頁(https://www.solarwinds.com/securityadvisory)進行更新至以下版本：
     - SolarWinds Orion Platform 2019.4 HF 6
     - SolarWinds Orion Platform 2020.2.1 HF 2
  2. 若未能即時完成修補或更新，建議可將FireEye所公開之SnortYaraClamAV或HXIOC規則部署於資安防護設備中，用以偵測或封鎖相關攻擊。連結如下：https://github.com/FireEye/sunburst_countermeasures
- 參考資料:
  1. https://www.solarwinds.com/securityadvisory
  2. https://github.com/FireEye/sunburst_countermeasures
  3. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
  4. https://www.ithome.com.tw/news/141651
  5. https://www.ithome.com.tw/news/141666
  6. https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1138

計算機與通訊中心
網路系統組 敬啟