張貼日期：2021/01/08

【資安漏洞預警】【更新影響平台與建議措施□SolarWinds Orion Platform部分版本存在後門程式，請儘速確認並進行版本更新

主旨：【資安漏洞預警】【更新影響平台與建議措施□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 NCCST-ANA-2020-0135
  - 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:
  1. SolarWinds Orion Platform 20194 HF 5 (版本號為version 2019.4.5200.9083)
  2. SolarWinds Orion Platform 2020.2 RC1 (版本號為version 2020.2.100.12219)
  3. SolarWinds Orion Platform 2020.2 RC2 (版本號為version 2020.2.5200.12394)
  4. SolarWinds Orion Platform 2020.2 (版本號為version 2020.2.5300.12432)
  5. SolarWinds Orion Platform 2020.2 HF 1 (版本號為version 2020.2.5300.12432)
- 建議措施:
  1. 根據美國國土安全部(DHS)在2020年12月30日所發布之緊急指令(21-02)補充指南，美國國家安全局(NSA)已確認SolarWinds Orion 2020.2.1 HF2版本並未含有惡意程式碼。在此建議有使用SolarWinds Orion Platform產品之機關，參考此更新資訊，聯絡設備維護廠商進行版本確認，並採取下列措施：
     1. 若為上述受影響版本，請完整移除後重新安裝SolarWinds Orion Platform 2020.2.1 HF 2版本。
     2. 若為其他非受影響版本，請更新至SolarWinds Orion Platform 2020.2.1 HF 2版本。
  2. 若未能即時完成修補或更新，建議可將FireEye所公開之Snort□Yara□ClamAV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://cyber.dhs.gov/ed/21-01/#supplemental-guidance
  2. https://www.solarwinds.com/securityadvisory
  3. https://github.com/FireEye/sunburst_countermeasures
  4. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
  5. https://www.ithome.com.tw/news/141651
  6. https://www.ithome.com.tw/news/141666
  7. https://www.ithome.com.tw/news/141971

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:20210108_01

Last update: **2021/01/08 10:55**