張貼日期：2021/12/20

【資安漏洞預警Apache Log4j存在更新修補程式後仍存在漏洞情況(新漏洞編號為CVE-2021-45046)請儘速確認並進行更新!

- 主旨說明：【資安漏洞預警Apache Log4j存在更新修補程式後仍存在漏洞情況(新漏洞編號為CVE-2021-45046)允許攻擊者遠端執行任意程式碼或洩露資訊，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-202112-0801
  - Apache Log4j是一個Java日誌記錄工具，因官方證實前次漏洞(CVE-2021-44228)之修補程式(2.15.0版)未完整修補漏洞(此漏洞警訊為技服中心於12/13發布之NCCST-ANA-2021-0000612警訊)，導致更新後之Log4j仍存在安全漏洞(新漏洞編號為CVE-2021-45046)攻擊者可藉由發送特製JNDI lookup訊息，利用漏洞進而遠端執行任意程式碼或洩露資訊。
- 影響平台:
  - Apache Log4j 2.0-beta9至215.0(含)版本，但不含2.12.2版本
- 建議措施:
  - 目前Apache Log4j官方網頁已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商進行版本確認並更新(Java 7使用者更新至Log4j 2.12.2版本Java 8使用者更新至Log4j 2.16.0版本)：https://logging.apache.org/log4j/2.x/security.html
- 參考資料:
  - https://logging.apache.org/log4j/2.x/security.html
  - https://nvd.nist.gov/vuln/detail/CVE-2021-45046

計算機與通訊中心
網路系統組 敬啟