

張貼日期：2021/12/15

【資安漏洞預警】Apache Log4j存在安全漏洞(CVE-2021-44228)請儘速確認並進行更新！

- 主旨說明：【資安漏洞預警】Apache Log4j存在安全漏洞(CVE-2021-44228)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 Apache Log4j存在安全漏洞(CVE-2021-44228)
 - Apache Log4j是一個Java日誌記錄工具，研究人員發現Log4j存在安全漏洞(CVE-2021-44228)攻擊者可藉由發送特製Log訊息，利用漏洞進而遠端執行任意程式碼。
- 影響平台：
 - Apache Log4j 2.0-beta9至214.1(含)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至Log4j 2.15.0版本：<https://logging.apache.org/log4j/2.x/security.html>
- 參考資料：
 1. <https://logging.apache.org/log4j/2.x/security.html>
 2. <https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability>
 3. <https://thehackernews.com/2021/12/extremely-critical-log4j-vulnerability.html>
 4. <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

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:20211215_01

Last update: **2021/12/15 08:50**

