張貼日期：2022/02/16

【資安漏洞預警】[更新檢測與修補說明]Apache Log4j存在Log4Shell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！

- 主旨說明：[更新檢測與修補說明]Apache Log4j存在Log4Shell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 NISAC-ANA-202202-0704□
  - 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:
  1. Apache Log4j 2.0-beta9至2.14.1(含)版本
  2. 漏洞檢測方式與相關技術細節詳見附件說明
     - 附件-行政院國家資通安全會報技術服務中心 Log4Shell(CVE-2021-44228)漏洞資訊與修補方式說明連結：https://cert.tanet.edu.tw/pdf/log4shell.pdf
- 建議措施:
  目前Cisco官方已針對這些漏洞釋出修復版本，請各機關可聯絡設備維護廠商或參考以下建議進行更新：
  1. 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，其中Java 8環境請更新至Log4j 2.17.0或之後版本□Java 7環境請更新至Log4j 2.12.3或之後版本□Java 6環境請更新至Log4j 2.3.1或之後版本：https://logging.apache.org/log4j/2.x/security.html
  2. 漏洞修補前，亦可透過以下步驟停用JNDI Lookup功能，以緩解此漏洞
     1. 針對log4j版本>=2.10的系統
        1. 請設定屬性□log4j2.formatMsgNoLookups=true□□
        2. 請設定環境變數□LOG4J_FORMAT_MSG_NO_LOOKUPS=true□□
     2. 針對log4j版本為2.0-beta9到2.100的系統
  3. 透過WAF對相關惡意語法進行過濾及阻擋
     使用對外防護設備針對JNDI之相關惡意攻擊行為設定規則進行阻擋,

     ```
     例如"$(jndi:ldap://"□
     ```

  4. 評估於Java伺服器增加以下設定以防止下載與執行可能具風險之惡意Java Class
     將com.sun.jndi.ldap.object.trustURLCodebase設定為false□使JNDI無法使用LDAP下載遠端Java Class□
- 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