張貼日期：2021/12/20

【資安漏洞預警Apache Log4j 出現重大遠程代碼執行漏洞。

- 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 數聯資安(ISSDU)情資編號ISSDU-ANA-202112-0002
  - 由於許多知名的大型應用系統如推特iCloudMinecraft等都使用了Log4j且這項漏洞極為容易被利用，已經出現攻擊行動的情況，被資安專家稱為近10年來最嚴重的漏洞。
  - Apache Log4j 2是基於Java的日誌框架，近日他們發布了新版本2.15.0，當中修補了一項遠端程式碼執行漏洞，用戶盡速升級最新版本。根據阿里雲安全團隊的說明Apache Log4j2的某些功能存在遞迴解析功能，而攻擊者可直接構造惡意請求，觸發遠端程式碼執行漏洞，並指出Apache Struts2Apache SolrApache DruidApache Flink都受影響。目前CVE漏洞編號CVE-2021-44228
- 影響平台:
  - Apache Log4j 2.15.0 版本之前的任何版本
- 建議措施:
  - 此問題已在 Log4J v2.15.0 中修復Apache 日誌服務團隊提供以下緩解建議：
    - 在以前的版本中，可以通過將系統屬性log4j2.formatMsgNoLookups設置為TRUE或從類路徑中刪除 JndiLookup 類來緩解這種行為。如果無法升級，請確保在客戶端和服務器端組件上都將參數Dlog4j2.formatMsgNoLookups設置為TRUE
    - 目前已有資安設備廠商已釋出相關攻擊特徵，分別有以下列表，建議擁有這些資安設備，將該特徵設定為阻擋，以避免遭外部攻擊者成功入侵。
      - Checkpoint:
        Apache Log4j Remote Code Execution (CVE-2021-44228)
      - Deep Security:
        Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)
      - Fidelis:
        FSS_CVE-2021-44228 - Apache Log4j Inject Request
      - Firepower:
        SERVER-OTHER Apache Log4j logging remote code execution attempt
        SERVER-APACHE Apache Log4j2 CVE- 2021-44228 Remote Code Execution Vulnerability
      - Fortigate:
        Apache.Log4j.Error.Log.Remote.Code.Execution
      - Palo Alto:
        Apache Log4j Remote Code Execution Vulnerability
      - Mcafee:
        UDS-HTTP: Apache Log4j2 Remote Code Execution Vulnerability
        HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
      - TippingPoint:
        HTTP: JNDI Injection in HTTP Request
      - IBM:
        HTTP_Log4J_JndiLdap_Exec
      - DDI:

HTTP_POSSIBLE_USERAGENT_RCE_EXPLOIT_REQUEST
CVE-2021-44228 - OGNL EXPLOIT - HTTP(REQUEST)
POSSIBLE HTTP HEADER OGNL EXPRESSION EXPLOIT - HTTP(REQUEST)
POSSIBLE HTTP BODY OGNL EXPRESSION EXPLOIT - HTTP (REQUEST) - Variant 2

- Sophos:
  SERVER-OTHER Apache Log4j logging remote code execution attempt
  SERVER-APACHE Apache Log4j2 CVE- 2021-44228 Remote Code Execution Vulnerability

- 參考資料:
  1. https://hominido.medium.com/iocs-para-log4shell-rce-0-day-cve-2021-44228-98019dd06f35
  2. https://nvd.nist.gov/vuln/detail/CVE-2021-44228
  3. https://www.ithome.com.tw/news/148307
  4. https://community.riskiq.com/article/505098fc/indicators
  5. https://github.com/advisories/GHSA-jfh8-c2jp-5v3q

計算機與通訊中心
網路系統組 敬啟