**Apache Log4j重大漏洞**

**事件時間軸**

2021年11月24日 阿里雲安全團隊向Apache通報Log4j遠端程式碼執行漏洞

2021年12月7日 Apache發布Log4j 2.15.0修補漏洞（當地12月6日）

2021年12月9日 阿里雲安全團隊發布Log4j的RCE漏洞預警

2021年12月10日 研究人員p0rz9在GitHub上揭露概念驗證攻擊程式

2021年12月11日 NIST NVD的CVE-2021-44228漏洞頁面公開（當地12月10日）

2021年12月14日 Apache發布Log4j 2.16.0（當地12月13日）

2021年12月15日 NIST NVD的CVE-2021-45046漏洞頁面公開（當地12月14日）

2021年12月18日 Apache發布Log4j 2.17.0（當地12月17日）

2021年12月20日 NIST NVD的CVE-2021-45105漏洞頁面公開（當地12月19日）

2021年12月29日 Apache發布Log4j 2.17.1（當地12月28日）

2021年12月29日 NIST NVD的CVE-2021-44832漏洞頁面公開（當地12月28日）

**說明漏洞**

編號為CVE-2021-44228的日誌框架系統Apache Log4j重大漏洞，肇因於某些功能存在遞迴解析功能，存在JNDI注入漏洞，而攻擊者可直接發出惡意請求，觸發遠端程式碼執行漏洞。

Log4Shell 漏洞出於 Log4j 裡有一個JNDI Lookup 功能，它是用來在執行階段對日誌中的文字紀錄進行加工後輸出，這本來在分析系統問題時很有用，不過同時也可以讓攻擊者有機可乘，例如刻意輸入下載軟體來執行的文字讓日誌記錄下來，就可以遠端執行任意程式碼。

**為什麼會有這樣的衝擊**

由於使用存在漏洞版本的Log4j，將無法防範攻擊者控制LDAP與其他JNDI有關的端點，一旦攻擊者掌握了事件記錄訊息或是參數，有可能在訊息探索啟用的情況下，從LDAP伺服器載入程式碼的管道，執行任意程式碼。

幾乎每個網路安全系統都會利用某種日誌框架進行紀錄，使得Log4j這類受歡迎的日誌框架影響廣泛。據了解，攻擊者只需傳送一則特殊的訊息到伺服器（含$的字串）就能觸發漏洞，遠端執行任意程式碼來控制目標伺服器，已出現攻擊行動的情況，漏洞波及面和危害程度均堪比2017年的永恆之藍(Eternal blue)漏洞，Apache軟體基金會也將Log4j漏洞的嚴重程度，評為最高的10分，任何人都可以從存在該漏洞的服務獲得電腦的完整存取權限。

**後續應變**

由於有多款軟體套件裡包含了Log4j，例如：Apache Struts2、Apache Solr、Apache Druid、Apache Flink，故應用系統的管理者需著手調查，是否採用名稱含有log4j-core的JAR檔案，假如此檔案有被引入使用，且為受影響的版本，[管理者應從Apache網站下載最新版本](https://logging.apache.org/log4j/2.x/download.html)，並儘速升級（2.15.0以上版本）。

若是無法更新Log4j，阿里雲也提到能使用較新版本的Java SDK（JDK），藉由限制JNDI漏洞利用的方式，來暫時緩解漏洞所帶來的風險。這些版本的SDK是6u211、7u201、8u191、11.0.1。再者，對於Log4j 2.10以上版本，亦可修改配置來達到緩解效果：將log4j2.formatMsgNoLookups的值設定為True，或將JndiLookup類別從classpath路徑刪除。

Log4j 1.x不會直接受到這個漏洞影響，但該版本產品生命週期已經結束（EOL），可能存在其他RCE漏洞且不會有修補程式，使用者仍應升級2.15.0以上版本。