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，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。