Apache Log4j 零時差漏洞已被開採

2021 年 12 月 11 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

賽門鐵克解決方案可防止有人企圖利用嚴重的 CVE-2021-44228 漏洞

2021 年 12 月 20 日更新：*Apache 軟體基金會發布了針對 Log4j 中第三個漏洞的修補程式。在發現上一版本 (2.16) 存在問題後，該軟體的 2.17.0 版於 12 月 17 日發布。Apache 表示，2.16 並不能完全防止查找評估中的無限遞迴，且容易受到 CVE-2021-45105（一種拒絕服務漏洞）的攻擊。*

2021 年 12 月 15 日更新：*Apache 已修補 Log4j 中的第二個漏洞。該漏洞 (CVE-2021-45046) 源於上一個漏洞 (CVE-2021-44228) 的修復程序並未能在所有情況下完全阻止漏洞利用。該修補功能已在 Log4j 版本 2.16.0 中提供。*

Apache Log4j 被發現了一個零時差漏洞（CVE-2021-44228），如果利用該漏洞，遠端攻擊者可以在有漏洞的系統上執行任意程式碼。此漏洞的攻擊代碼（稱為 Log4Shell）已被公開分享，多個攻擊者已經在嘗試利用此漏洞。

問：賽門鐵克能否防止漏洞刺探攻擊？

答：是的，賽門鐵克產品將會透過以下多種偵測技術來防止此漏洞利用的企圖：

基於行為偵測技術(Snoar)的防護：

- SONAR.Maljava!g7
- SONAR.Ransomware!g1
- SONAR.Ransomware!g31
- SONAR.Ransomware!g32
- SONAR.SuspLaunch!g184
- SONAR.SuspLaunch!g185

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen106
- CL.Suspexec!gen107
- CL.Suspexec!gen108
- Linux.Kaiten
- Miner.XMRig!gen2
- Ransom.Khonsari

- Ransom.Tellyouthepass
- Ransom.Tellyouthepa!g1
- Ransom.Tellyouthepa!g2
- Trojan Horse
- Trojan.Maljava

基機器學習的防禦技術：

- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Attack: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j CVE-2021-45046
- Attack: Malicious LDAP Response
- Audit: Log4j2 RCE CVE-2021-44228
- Audit: Malicious LDAP Response
- Audit: Suspicious Java Class File Executing Arbitrary Commands

基於安全強化政策(適用於使用DCS：Data Center Security)， 針對此漏洞為伺服器工作負載提供了一系列保護：

- 可疑程序執行：預防政策集可防止惡意軟體被植入或在系統上執行。DCS 強化的 Linux 伺服器可防止從臨時或其他可寫位置執行惡意軟體，攻擊者使用這種技術在所報導的 log4shell 漏洞利用中植入 XMRig 等加密程式。
- 查看基於 log4j 應用程序沙箱的 Linux 代理執行清單，並新增，例如：*/curl、*/wget 等其他工具。攻擊者使用這些工具從受害者的 log4j 應用程序連接到外部 C2 伺服器以下載額外的有效籌載。
- DCS 的應用程式沙箱，可以保護 Windows 和 Linux 使用就地取材工具和篡改關鍵系統服務和資源的可疑程序執行。
- 網路控制：能夠阻止與網際網路的離埠連線，並限制來自伺服器工作負載和使用 log4j2 的容器化應用程序到內部可信系統所需的 LDAP、http 和其他流量。
- 檢測策略：系統攻擊檢測：Baseline_WebAttackDetection_Generic_MaliciousUserAgent 規則應更新為包含 *jndi:* 透過選擇字串 jndi:ldap、jndi:rmi、jndi:dns 等使用可疑的 jndi 查找嘗試警告惡意伺服器請求。確保設置 IDS Web 攻擊檢測選項中的 Web 伺服器存取日誌文件的路徑。應該為每個 log4j 應用程序日誌文件新增類似的自定義文本日誌規則。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

我們的 Webpulse (網頁脈衝) 常態監視的流量也包含 Log4jShell 漏洞來提供另一層級的保護。

問：此漏洞的意義是什麼？

答：Apache Log4j是一個基於java的日誌記錄工具。它廣泛用於雲和企業軟體服務。事實上，在正式發布修補程式之前就發現漏洞利用只會加劇威脅的嚴重性。

問：該漏洞是否已修補？

答：是的，建議使用者立即更新到版本2.15.0。Apache也為先前版本的使用者提供了緩解建議。

問：此漏洞是否在現實網路環境中被利用？

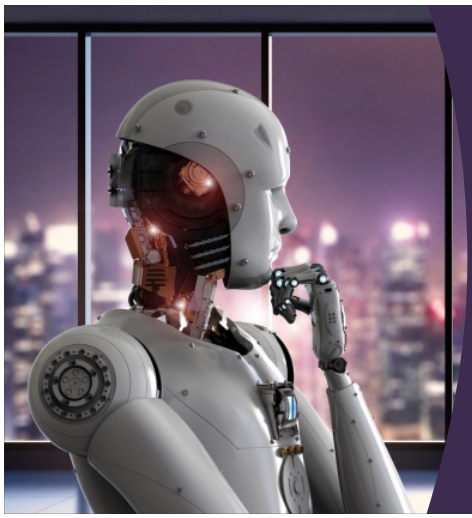
答：是的。漏洞程式碼是可公開取得，並且有多個關於嘗試利用漏洞的報告。迄今為止，活動似乎主要集中在挖礦殭屍網路上，但所有類型的攻擊者試圖利用這種漏洞只是時間早晚的問題。

保護／緩解

有關最新的防護更新，請訪問賽門鐵克防護公告。

更多資訊

1. 賽門鐵克對 Log4j 漏洞的回應
2. 賽門鐵克線上安全顧問諮詢



關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apache-log4j-zero-day
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2021/12

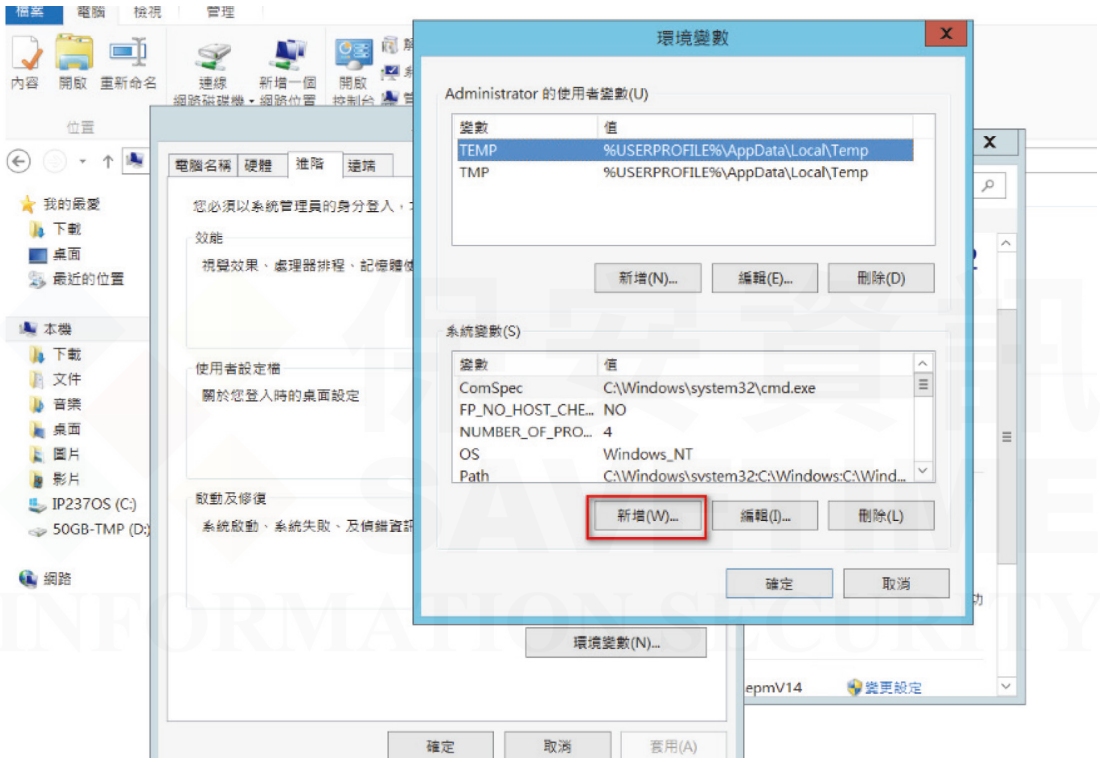
◎ 本漏洞可能會與賽門鐵克軟體有關的說明，請參考以下原廠的說明：

https://support.broadcom.com/security-advisory/content/security-advisories/Symantec-Security-Advisory-for-Log4j-2-CVE-2021-44228-Vulnerability/SYMSA19793

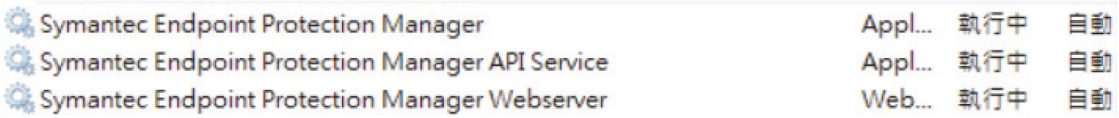
◎ SEPM 修正的知識庫請參考：

https://knowledge.broadcom.com/external/article/230359

◎ 以下為詳細操作步驟請參考如下：



然後重新啟動 SEPM 系統服務



更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588