林鉦烜

寄件者: 行政院國家資通安全會報技術服務中心 <ncert@nccst.nat.gov.tw>
寄件日期: 2021年12月22日星期三 下午 1:36
收件者: moe_infosec@mail.moe.gov.tw; ghfj5678@chtsecurity.com; esora@mail.moe.gov.tw
主旨: [External] [緊急應處警訊] 國家資通安全會報技術服務中心 (事件編號：NCCST-ALT-2021-0000021)
簽名者: ncert@nccst.nat.gov.tw

行政院國家資通安全會報技術服務中心

緊急應處警訊

發布編號	NCCST-ALT-2021-0000021	發布時間	Wed Dec 22 13:12:09 CST 2021
事件類型	其他	發現時間	Tue Dec 21 00:00:00 CST 2021
事件主旨	Apache Log4j 安全漏洞(CVE-2021-44228 與 CVE-2021-45046)更新調查		
事件描述	Apache Log4j 是一套 Java 的日誌紀錄框架工具，開發人員可透過該框架對 Java 程式的運作情形進行日誌紀錄，近日研究人員發現 Log4j 其存在安全漏洞(CVE-2021-44228 與 CVE-2021-45046)，受影響版本為 2.0-beta9 至 2.15.0，已有駭客利用上述漏洞發起攻擊活動，為掌握各機關影響情形，請各機關儘速調查 Apache Log4j 使用與更新情況，彙整自身及所屬、轄內及所管公務機關更新情形，並於 2022 年 1 月 4 日前至通報應變網站回覆。		
因應對策	1. 本次調查範圍含機關及所屬機關，請調查自身及各所屬機關是否已完成 Log4shell 漏洞更新作業 2. 檢視資訊設備/服務受影響狀況： (1) 美國資安暨關鍵基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）已於 Github 公告「Apache Log4j 漏洞的處理修復指南」(https://github.com/cisagov/log4j-affected-db)提供受影響之產品與服務 (2) 技服中心參考美國卡內基美隆大學 CERT/CC 提供之檢測工具，彙整「Apache log4shell 漏洞掃描工具使用說明」於通報應變網站(通報應變網站首頁→文件下載)，機關可逕行下載閱讀並確認受影響情況。 3. Apache Log4shell 攻擊特徵： 如機關於網站伺服器或其他資安防護設備日誌發現以下字串，請進一步檢視是否已遭入侵成功 "jndi:ldap:/ "jndi:rmi:/ "jndi:ldaps:/		

	"jndi:dns:/ "jndi:nis:/ "jndi:nds:/ "jndi:corba:/ "jndi:iiop:/ "jndi:${ "${jndi: ${lower: ${upper: ${env: ${sys: ${java: "${date: ${::-j"
參考資料	1. 技服中心警訊「NCCST-ANA-2021-0000612」、「NCCST-ANA-2021-0000637」 2. https://github.com/cisagov/log4j-affected-db 3. https://github.com/CERTCC/CVE-2021-44228_scanner 4. https://logging.apache.org/log4j/2.x/
調查說明	資安研究團隊於 2021 年 12 月初發現 Java 日誌記錄工具(Apache Log4j) 存在安全漏洞(CVE-2021-44228 與 CVE-2021-45046)，遞迴解析功能存在 JNDI 注入漏洞，攻擊者可直接發出惡意請求，觸發遠端程式碼執行漏洞。由於已有駭客利用上述漏洞發起攻擊活動，為掌握各機關影響情形，請各機關儘速調查 Apache Log4j 使用與更新情況，彙整自身及所屬、轄內及所管公務機關更新情形，並於 2022 年 1 月 4 日前至通報應變網站回覆。 【事件調查表填報說明】 1. 警訊內容回報項目：請針對機關內部資訊設備/服務處理情況說明 「機關處置說明」：可針對機關及所屬針對受影響資訊設備/服務目前處置現況補充說明

	「預計處理完成時間」：機關及所屬完成資訊設備/服務更新時間，若機關及所屬皆不在影響範圍，則填報調查完成時間 「此警訊是否已完成」：未完成自身及所屬機關受影響調查前，皆可編輯本事件調查表 2. 機關使用資訊設備/服務更新版本調查：請說明機關使用 Log4j 工具之資訊設備/服務更新版本與更新情況 3. 所屬公務機關調查情況：請協助調查所屬公務機關使用 Log4j 工具之資訊設備/服務更新版本與更新情況
問卷複本	否
回報日期	Tue Jan 04 23:59:59 CST 2022

此事件須要填寫事件調查表，請儘速登入通報應變網站填寫並於[回報日期]內完成警訊處理。
附件密碼請登入通報應變網站檢視(警訊資料查詢→事件調查表)，若發現系統有遭入侵情事，須另外進行通報。
請貴單位資安人員點選下列連結填寫事件調查表。
填寫事件調查表

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告內容有疑問或有關於此事件之建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。
地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw