張貼日期：2026/05/13

【漏洞預警】Apache ActiveMQ Classic存在高風險安全漏洞(CVE-2026-34197)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】Apache ActiveMQ Classic存在高風險安全漏洞(CVE-2026-34197)，請儘速確認並進行修補

- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-200-202604-00000011
  - 研究人員發現Apache ActiveMQ Classic存在不當輸入驗證(Improper Input Validation)與程式碼注入(Code Injection)漏洞(CVE-2026-34197)，因Web Console暴露之Jolokia JMX-HTTP介面允許執行特定操作且缺乏輸入驗證，使已通過身分鑑別之遠端攻擊者可傳入惡意參數，進而執行任意程式碼。此漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
  - Apache ActiveMQ Broker 5.19.4(不含)以前版本
  - Apache ActiveMQ Broker 6.0.0至6.2.3(不含)版本
  - Apache ActiveMQ 5.19.4(不含)以前版本
  - Apache ActiveMQ 6.0.0至6.2.3(不含)版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：
    https://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-34197
  2. https://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt

---

計算機與通訊中心
網路系統組 敬啟