張貼日期：2023/11/14

【漏洞預警】Apache ActiveMQ存在高風險安全漏洞(CVE-2023-46604)請儘速確認並進行更新!

- 主旨說明：Apache ActiveMQ存在高風險安全漏洞(CVE-2023-46604)，允許攻擊者於未經身分鑑別之情況下遠端執行任意程式碼，請儘速確認並進行更新!
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202311-00000033
  - 研究人員發現Apache ActiveMQ之OpenWire協定存在未受信任之資料反序列化(Deserialization of Untrusted Data)漏洞(CVE-2023-46604)，允許攻擊者於未經身分鑑別之情況下發送惡意字串，使受影響系統進行物件反序列化時執行惡意字串，進而利用此漏洞執行任意程式碼。該漏洞目前已遭駭客利用，請儘速確認並進行更新。
- 影響平台：
  - ActiveMQ 5.17.0至5.17.5版本
  - ActiveMQ 5.16.0至5.16.6版本
  - ActiveMQ 5.18.0至5.18.2版本
  - ActiveMQ Artemis 2.31.1(含)以下版本
  - Apache ActiveMQ Legacy OpenWire Module 5.16.0至5.16.6版本
  - Apache ActiveMQ Legacy OpenWire Module 5.17.0至5.17.5版本
  - ActiveMQ 5.15.15(含)以下版本
  - Apache ActiveMQ Legacy OpenWire Module 5.8.0至5.15.15版本
  - Apache ActiveMQ Legacy OpenWire Module 5.18.0至5.18.2版本
- 建議措施：
  - 目前Apache官方已針對此漏洞釋出更新程式，請各機關儘速進行版本確認與更新：
    1. ActiveMQ請升級至5.15.16、5.16.7、5.17.6及5.18.3版本
    2. ActiveMQ Artemis請升級至2.31.2版本
- 參考資料：
  1. https://activemq.apache.org/news/cve-2023-46604
  2. https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt
  3. https://nvd.nist.gov/vuln/detail/CVE-2023-46604
  4. https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10785
  5. https://www.ithome.com.tw/news/159685
  6. https://socradar.io/critical-rce-vulnerability-in-apache-activemq-is-targeted-by-hellokitty-ransomware-cve-2023-46604/

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20231114_01

Last update: **2023/11/14 10:19**