

張貼日期：2020/05/27

# 【資安漏洞預警】Apache Tomcat伺服器存在安全漏洞(CVE-2020-9484)允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

主旨：【資安漏洞預警】Apache Tomcat伺服器存在安全漏洞(CVE-2020-9484)允許攻擊者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 資安訊息警訊 NISAC-ANA-202005-0685
  - 研究人員發現Apache Tomcat伺服器存在反序列化漏洞(CVE-2020-9484)遠端攻擊者可對符合特定條件(如啟用PersistenceManager的FileStore功能，且PersistenceManager的sessionAttributeValueClassNameFilter參數設為null等)之目標設備發送特製請求，利用此漏洞進而執行任意程式碼。
- 影響平台：

受影響Tomcat伺服器版本如下：

  - Apache Tomcat 10.0.0-M4(含)以前版本
  - Apache Tomcat 9.0.34(含)以前版本
  - Apache Tomcat 8.5.54(含)以前版本
  - Apache Tomcat 7.0.103(含)以前版本
- 建議措施：
  1. 目前Apache Tomcat官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商進行版本確認並將設備更新至以下版本：
    - Apache Tomcat 10.0.0-M5(含)以後版本
    - Apache Tomcat 9.0.35(含)以後版本
    - Apache Tomcat 8.5.55(含)以後版本
    - Apache Tomcat 7.0.104(含)以後版本
  2. 各版本對應之官方公告連結如下：
    1. <https://tomcat.apache.org/security-10.html>
    2. <https://tomcat.apache.org/security-9.html>
    3. <https://tomcat.apache.org/security-8.html>
    4. <https://tomcat.apache.org/security-7.html>
- 參考資料：
  1. <https://tomcat.apache.org/security-10.html>
  2. <https://tomcat.apache.org/security-9.html>
  3. <https://tomcat.apache.org/security-8.html>
  4. <https://tomcat.apache.org/security-7.html>
  5. <https://www.csa.gov.sg/singcert/alerts/al-2020-015>

---

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/announcement:20200527\\_02](https://net.nthu.edu.tw/netsys/announcement:20200527_02)

Last update: **2020/05/27 11:01**

