張貼日期：2020/04/22

【資安漏洞預警Tomcat 網站伺服器具有資訊外洩的漏洞(CVE-2020-1938 and CNVD-2020-10487)請各單位儘速確認並更新修補

主旨：【資安漏洞預警Tomcat 網站伺服器具有資訊外洩的漏洞(CVE-2020-1938 and CNVD-2020-10487)請各單位儘速確認並更新修補。

- 內容說明：
  - 轉發 ANA事件單通知:TACERT-ANA-2020042112041515
  - Apache Tomcat網站伺服器在版本9.x8.x與7.x中，存在漏洞(CVE-2020-1938 and CNVD-2020-10487)該漏洞可能允許讀寫Tomcat的webapp目錄中的文件。
  - Apache Tomcat網站伺服器是可運行Java代碼的開源Web服務器。由於所使用的AJP(Apache JServ Protocol)協議設計上存在缺陷，攻擊者可利用預設開啟且未設定外部存取的AJP服務(預設為8009通訊埠)，達到遠端指令執行(Romote Code Execution, RCE)之目的；查看、更改、刪除數據或建立具有完整權限的新帳戶等。此外，如果網站應用程序允許用戶上傳文件，則攻擊者可能會將包含惡意代碼的文件上傳到伺服器，使該系統成為惡意程式下載站(Download Site)
- 影響平台:
  - 使用Tomcat作為網站伺服器，且版本為:
    Apache Tomcat 9.x
- 建議措施:
  1. 目前Apache Tomcat官方網站 (http://tomcat.apache.org/) 已針對此弱點於月11日與14日針對版本9.x8.x與7.x版發布更新修補。請各機關儘速更新修補，升級至9.0.31、8.5.51與7.0.100版本。
  2. 如果不需要Tomcat 網站伺服器全權公開連線，請將Apache JServ協議AJP服務作外部存取的權限控制，以避免惡意攻擊。
- 參考資料:
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1938

計算機與通訊中心
網路系統組 敬啟

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

Permanent link:
http://net.nthu.edu.tw/netsys/mailing:announcement:20200422_02

Last update: **2020/04/22 09:44**