張貼日期：2022/04/08

【資安漏洞預警Spring Framework存在Spring4shell高風險安全漏洞(CVE-2022-22965)請儘速確認並進行更新！

- 主旨說明Spring Framework存在Spring4shell高風險安全漏洞(CVE-2022-22965)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 NISAC-ANA-202204-0125
  - Spring Framework為輕量級Java開源框架，研究人員發現Spring Framework未正確處理資料繫結(Data binding)導致存在Spring4shell安全漏洞(CVE-2022-22965)攻擊者可針對同時滿足下列5個條件之目標主機，利用此漏洞遠端執行任意程式碼，此外，基於Spring Framework所衍生出之Spring Boot亦存在此漏洞。
    1. 使用Spring Framework 5.3.0~5.3.17、5.2.0~5.2.19或更舊之版本
    2. 使用JDK 9(含)以上版本
    3. 使用Apache Tomcat做為Servlet容器
    4. 網站專案使用Java web archive(WAR)方式封裝，並部署於獨立之Tomcat實體
    5. Tomcat具有spring-webmvc或spring-webflux相依性
- 影響平台:
  - Spring Framework 5.2.20(不含)以前版本
  - Spring Framework 5.3.18(不含)以前版本
  - Spring Boot 2.5.12(不含)以前版本
  - Spring Boot 2.6.6(不含)以前版本
- 建議措施:
  1. Spring官方網頁(https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement) 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與更新：
     1. 更新Spring Framework至5.2.20或5.3.18以上版本
     2. 更新Spring Boot至2.5.12或2.6.6以上版本
  2. 若無法更新至最新版本，請參考Spring官方網頁之Suggested Workarounds一節，採取下列緩解措施：
     1. 升級Apache Tomcat至8.5.78、9.0.62或100.20以上版本
     2. 降版至Java 8
     3. 透過全域設定關閉特定欄位之綁定功能
- 參考資料:
  1. https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
  2. https://spring.io/blog/2022/04/01/spring-framework-rce-mitigation-alternative
  3. https://www.microsoft.com/security/blog/2022/04/04/springshell-rce-vulnerability-guidance-for-protecting-against-and-detecting-cve-2022-22965/

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:20220408_02

Last update: **2022/04/08 08:38**