張貼日期：2020/07/16

【資安漏洞預警□SAP NetWeaver AS Java存在安全漏洞，請儘速確認並進行更新

主旨：【資安漏洞預警□SAP NetWeaver AS Java存在安全漏洞(CVE-2020-6287)□允許攻擊者遠端執行任意系統指令，請儘速確認並進行更新

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 (NCCST-ANA-G2020-0284)□
  - 研究人員發現SAP NetWeaver Application Server (AS) Java之LM Configuration Wizard存在缺乏有效的身分認證(lack of authentication)安全漏洞(CVE-2020-6287)□遠端攻擊者可對目標設備發送特製請求，利用此漏洞建立管理者身分之帳號進而執行任意系統指令。
- 影響平台:
  SAP NetWeaver AS Java為以下版本：
  - 7.30、7.31、7.40及7.50
- 建議措施:
  目前微軟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或參考以下建議進行更新：
  1. 目前SAP官方已針對此弱點釋出更新程式，請各機關聯絡設備維護廠商進行版本確認，參考連結：https://launchpad.support.sap.com/#/notes/2934135
  2. 若無法立即更新，可參考公告應先關閉LM Configuration Wizard服務進行緩解，參考連結：https://launchpad.support.sap.com/#/notes/2939665
- 參考資料:
  1. https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675
  2. https://zh-tw.tenable.com/blog/cve-2020-6287-critical-vulnerability-in-sap-netweaver-application-server-java-disclosed-recon
  3. https://us-cert.cisa.gov/ncas/alerts/aa20-195a

計算機與通訊中心
網路系統組 敬啟