行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2020-0072	發布時間	Wed Jul 15 16:27:45 CST 2020
事件類型	漏洞預警	發現時間	Wed Jul 15 00:00:00 CST 2020
警訊名稱	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	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		
影響等級	高		
建議措施	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		

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw