教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026091808091414	發佈時間	2026-09-18 08:50:15
事故類型	ANA-漏洞預警	發現時間	2026-09-18 08:50:15
影響等級	低		

[主旨說明:]【漏洞預警】SAP 針對旗下多款產品發布重大資安公告

[內容說明:]

轉發　台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202609-00000019

SAP 發布九月份例行更新，共修補 20 項漏洞，其中 4 項屬於高風險資安漏洞(CVE-2026-44756，CVSS：10.0、CVE-2026-58240，CVSS：9.8、CVE-2026-76969，CVSS：9.4 和 CVE-2026-66768，CVSS：9.0)。

CVE-2026-44756，Extended Passport Protocol (EPP)處理庫中存在記憶體安全漏洞，在特定條件下，未經身分驗證的攻擊者可利用特製的網路請求，導致程式出現未定義行為並異常終止。

CVE-2026-58240，SAP NetWeaver Message Server 在註冊過程中對內部應用伺服器元件的真實性驗證不足，未經身分驗證的攻擊者若有網路存取權限，可能在應用環境中執行未經授權的操作。

CVE-2026-76969，@sap/cds-mtxs NPM library 對啟用可擴展性的 multitenant CAP 應用中使用的某些功能未進行充分檢查，未經身分驗證的攻擊者可利用特製的請求獲取敏感憑證。

CVE-2026-66768，SAP GUI for Java 對某些從連接的後端系統呼叫函數未能正確執行信任等級策略，低權限的攻擊者可利用此漏洞，透過操縱連接的後端系統導致在受害者機器上執行任意命令。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

SAP Extended Passport (EPP) Processing KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, 8.04, WEBDISP 9.16, 9.18, 9.19, 9.20, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16, 9.18, 9.19, 9.20 版本

SAP NetWeaver (Message Server) KERNEL 9.16, 9.18, 9.19, 9.20 版本

sap/cds-mtxs 特定版本

SAP NetWeaver (SAP GUI for Java) BC-FES-JAV 8.10 版本

[建議措施:]

根據官方網站釋出的解決方式進行修補 https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html?isu_page=1

[參考資料:]

1. https://www.twcert.org.tw/tw/cp-169-11207-b9e4b-1.html