教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026071601073131	發佈時間	2026-07-16 13:24:31
事故類型	ANA-漏洞預警	發現時間	2026-07-16 13:24:31
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-200-202607-00000008

【CVE-2026-44747，CVSS：9.9】 SAP NetWeaver Application Server ABAP 允許經過身分驗證的攻擊者利用記憶體管理的邏輯錯誤造成記憶體損壞，導致未經授權的資料存取、修改或系統無法使用。

【CVE-2026-27690，CVSS：9.1】 SAP Approuter 中存在 HTTP 請求走私漏洞(HTTP Request Smuggling vulnerability)，未經身分驗證的攻擊者可以發送精心設計的 HTTP 請求，導致請求回應不同步，導致洩漏用戶回應資料，並影響系統無法使用。

【CVE-2026-44761，CVSS：9.1】 SAP Commerce Cloud 可能保留範例 OAuth2 用戶端，其中包含公開記錄的範例憑證，這些憑證源自 SAP 說明入口網站文件中提供的範例設定。未經身份驗證的攻擊者可利用公開憑證來取得有效的 token，並呼叫某些 API 讀取和修改資料。

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 NetWeaver Application Server ABAP Version(s) - KRNL64NUC 7.22, 722EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53. 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 9.19, 9.20

SAP Approuter Version(s) - SAP Approuter node.js package < 20.10.0

SAP Commerce Cloud Version(s) - HY_COM 2205, COM_CLOUD 2211, 2211-JDK21

[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/july-2026.html