教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026081404084040	發佈時間	2026-08-14 16:11:41
事故類型	ANA-漏洞預警	發現時間	2026-08-14 16:11:41
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-200-202608-00000010

SAP 發布八月份例行更新，其中 4 項屬於高風險資安漏洞。

【CVE-2026-58231，CVSS：10.0】 SAP Commerce Cloud 允許未經身分驗證的攻擊者濫用預設身分驗證用戶端，向某些缺乏完整驗證的函數提交精心設計的輸入，若成功利用此漏洞可能導致任意程式碼執行並破壞內部元件。

【CVE-2026-34265，CVSS：9.8】 SAP NetWeaver and ABAP Platform 允許未經身分驗證的攻擊者可利用 DIAG 協定解析中的邏輯錯誤，可能導致記憶體損壞、洩漏敏感系統資訊或系統崩潰。

【CVE-2026-44758，CVSS：9.1】 SAP Manufacturing Integration and Intelligence 允許具有高權限的攻擊者向某些受影響的功能提交精心設計的輸入，在未經充分驗證的情況下，若攻擊者功能利用此漏洞可在底層作業系統上執行任意命令。

【CVE-2026-58243，CVSS：8.8】 SAP ABAP Developer Tools 的某些功能未執行必要的授權檢查，導致權限較低的攻擊者可對 SAP NetWeaver AS ABAP 執行未經授權的資料庫操作，若成功利用此漏洞可能導致攻擊者讀取敏感資料、修改應用程式資料並中斷合法用戶訪問。

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:]

【CVE-2026-58231】 SAP Commerce Cloud (Data Hub Adapter) Version(s) - COM_CLOUD 2211, 2211-JDK21

【CVE-2026-34265】 SAP NetWeaver and ABAP Platform Version(s) - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.22EXT2, 7.22EXT3, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16 9.18, 9.19, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16, 9.18, 9.19

【CVE-2026-44758】 SAP Manufacturing Integration and Intelligence Version(s) - XMII 15.4, 15.5

【CVE-2026-58243】 SAP ABAP Developer Tools Version(s) - SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816, SAP_BASIS 918, SAP_BASIS 920

[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/august-2026.html?isu_page=1
[參考資料:] 1. https://www.twcert.org.tw/tw/cp-169-11102-6a741-1.html