

## ANA事件單通知:TACERT-ANA-2025071009072525【漏洞預警】SAP針對旗下多款產品發布重大資安公告

### 教育機構ANA通報平台

|      |                             |      |                     |
|------|-----------------------------|------|---------------------|
| 發佈編號 | TACERT-ANA-2025071009072525 | 發佈時間 | 2025-07-10 09:26:25 |
| 事故類型 | ANA-漏洞預警                    | 發現時間 | 2025-07-10 09:26:25 |
| 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 TWCERTCC-200-202507-00000006

【CVE-2025-42967，CVSS：9.9】此漏洞存在於SAP S/4HANA 和 SAP SCM Characteristic Propagation，允許具有使用者權限的攻擊者利用程式碼建立文件，可能完全控制受影響的SAP系統。

【CVE-2025-42980，CVSS：9.1】該漏洞存在於SAP NetWeaver Enterprise Portal Federated Portal Network，允許特權使用者上傳不受信任或惡意內容，這些內容反序列化後可能導致主機系統受損害。

【CVE-2025-42964，CVSS：9.1】該漏洞存在於SAP NetWeaver Enterprise Portal Administration，允許特權使用者上傳不受信任或惡意內容，這些內容反序列化後可能導致主機系統受損害。

【CVE-2025-42966，CVSS：9.1】SAP NetWeaver XML Data Archiving服務存在Java反序列化漏洞，允許經過驗證且擁有管理者權限的攻擊者，利用精心設計的序列化Java物件影響應用程式的機密性、完整性及可用性。

【CVE-2025-42963，CVSS：9.1】SAP NetWeaver Application server的Java Log存在Java反序列化漏洞，允許經過驗證且擁有管理者權限的攻擊者，可完全控制受影響的系統，嚴重影響應用程式和主機環境的機密性、完整性及可用性。

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:]

- SCMAPO 713,714
- S4CORE 102,103,104
- S4COREOP 105,106,107,108
- SCM 700,701,702,712
- EP-RUNTIME 7.50
- J2EE-APPS 7.50
- LMNWABASICAPPS 7.50

[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-2025.html>

[參考資料:]

<https://www.twcert.org.tw/tw/cp-169-10236-5d1e9-1.html>

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：[service@cert.tanet.edu.tw](mailto:service@cert.tanet.edu.tw)