

## ANA事件單通知:TACERT-ANA-2025081409081010【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-2025081409081010 | 發佈時間 | 2025-08-14 09:53:10 |
| 事故類型 | ANA-漏洞預警                    | 發現時間 | 2025-08-14 09:53:10 |
| 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-200-202508-00000009

【CVE-2025-42957，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RFC公開功能模組的漏洞，將任意ABAP程式碼注入系統，從而繞過必要的授權檢查。

【CVE-2025-42950，CVSS：9.9】該漏洞存在於SAP Landscape Transformation (SLT)，允許具有使用者權限的攻擊者透過RFC公開功能模組的漏洞，將任意ABAP程式碼注入系統，從而繞過必要的授權檢查。

【CVE-2025-42951，CVSS：8.8】SAP Business One (SLD) 存在授權漏洞，允許經過驗證的攻擊者透過呼叫對應的API取得資料庫的管理員權限。

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 S/4HANA (Private Cloud or On-Premise) S4CORE 102, 103, 104, 105, 106, 107, 108版本
- SAP Landscape Transformation (Analysis Platform) DMIS 2011\_1\_700, 2011\_1\_710, 2011\_1\_730, 2011\_1\_731, 2011\_1\_752, 2020 版本
- SAP Business One (SLD) B1\_ON\_HANA 10.0, SAP-M-BO 10.0 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/august-2025.html>

[參考資料:]

<https://www.twcert.org.tw/tw/cp-169-10324-fd8bf-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)