

張貼日期：2025/07/11

【漏洞預警】SAP針對旗下多款產品發布重大資安公告

- 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。

- 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>

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailin:announcement:20250711_02 

Last update: **2025/07/11 15:17**