張貼日期：2025/09/12

【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-200-202509-00000006
  - 【CVE-2025-42944】(CVSS:10.0) SAP NetWeaver 存在反序列化漏洞。未經驗證的攻擊者可透過 RMI-P4 模組，向對外開放的連接埠傳送惡意負載，進而執行任意作業系統命令，對應用程式的機密性、完整性及可用性構成潛在威脅。
  - 【CVE-2025-42922】(CVSS:9.9) SAP NetWeaver AS Java 存在允許經過管理身分驗證的攻擊者上傳任意檔案的漏洞，可能導致系統的機密性、完整性和可用性造成破壞。
  - 【CVE-2025-42958】(CVSS:9.1) IBM i-series 的SAP NetWeaver 應用程式缺少身分驗證檢查，允許高權限的未經授權使用者讀取、修改或刪除敏感資料，並進一步存取管理功能或以特權權限操作，對應用程式的機密性、完整性與可用性構成重大風險。
  - 【CVE-2025-42933】(CVSS:8.8) 當用戶透過 SAP Business One 原生用戶端登入時，由於 SLD 後端服務未對部分 API 強制使用適當的加密機制，導致敏感憑證可能在 HTTP 回應主體中外洩，進而嚴重影響應用程式的機密性、完整性與可用性。
- 影響平台:
  - 【CVE-2025-42944】 SAP Netweaver (RMI-P4) SERVERCORE 7.50
  - 【CVE-2025-42922】 SAP NetWeaver AS Java J2EE-APPS 7.50
  - 【CVE-2025-42958】 SAP NetWeaver KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54
  - 【CVE-2025-42933】 SAP Business One (SLD) B1_ON_HANA 10.0, SAP-M-BO 10.0
- 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/september-2025.html
- 參考資料:
  1. SAP Security Patch Day - September 2025【
     https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2025.html
  2. CVE-2025-42944【 https://www.cve.org/CVERecord?id=CVE-2025-42944
  3. CVE-2025-42922【 https://www.cve.org/CVERecord?id=CVE-2025-42922
  4. CVE-2025-42958【 https://www.cve.org/CVERecord?id=CVE-2025-42958
  5. CVE-2025-42933【 https://www.cve.org/CVERecord?id=CVE-2025-42933

計算機與通訊中心
網路系統組 敬啟f

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

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20250912_04

Last update: **2025/09/12 15:18**