POSTING DATE: 2025/12/17

[VULNERABILITY ALERT] SAP Releases Critical Security Advisories for 2 Products (CVE-2025-42928) (CVE-2025-42880)

- Subject: [VULNERABILITY ALERT] SAP Releases Critical Security Advisories for 2 Products (CVE-2025-42928) (CVE-2025-42880)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202512-00000005
  - [CVE-2025-42928, CVSS: 9.1] This is a deserialization vulnerability. A user with high privileges could exploit this vulnerability to trigger a Remote Code Execution (RCE) attack, affecting the confidentiality, integrity, and availability of the system.
  - [CVE-2025-42880, CVSS: 9.9] Due to a lack of input filtering mechanisms, SAP Solution Manager allows an authenticated attacker to inject malicious code when calling remote-enabled function modules, potentially affecting the confidentiality, integrity, and availability of the system.
- Affected Platforms:
  - [CVE-2025-42928] SAP jConnect - SDK for ASE SYBASE_SOFTWARE_DEVELOPER_KIT versions 16.0.4, 16.1
  - [CVE-2025-42880] SAP Solution Manager ST version 720
- Recommended Actions:
  - Apply patches according to the solutions released on the official website: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2025.html

---

Computer and Communication Center
Network Systems Division, Respectfully