Date Posted: 2025/09/12

[Vulnerability Alert] SAP Releases Major Security Advisory for Multiple Products

- Subject: [Vulnerability Alert] SAP Releases Major Security Advisory for Multiple Products
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202509-00000006
  - [CVE-2025-42944, CVSS: 10.0] SAP NetWeaver has a deserialization vulnerability. An unauthenticated attacker can exploit the RMI-P4 module to send a malicious payload to an exposed port, leading to arbitrary operating system command execution, posing a potential threat to the confidentiality, integrity, and availability of the application.
  - [CVE-2025-42922, CVSS: 9.9] SAP NetWeaver AS Java has a vulnerability that allows authenticated attackers with administrative privileges to upload arbitrary files, which may lead to a compromise of the system's confidentiality, integrity, and availability.
  - [CVE-2025-42958, CVSS: 9.1] The SAP NetWeaver application on IBM i-series lacks authentication checks, allowing highly-privileged unauthorized users to read, modify, or delete sensitive data, and further access administrative functions or operate with privileged permissions, posing a significant risk to the application's confidentiality, integrity, and availability.
  - [CVE-2025-42933, CVSS: 8.8] When users log in through the SAP Business One native client, the SLD backend service does not enforce proper encryption mechanisms for some APIs, which may lead to sensitive credentials leaking in the HTTP response body, severely impacting the application's confidentiality, integrity, and availability.
- Affected Platforms:
  - SAP NetWeaver
  - SAP NetWeaver AS Java
  - SAP Business One
- Recommended Action:
  - Please refer to the official security advisory for the solution.
- References:
  - https://www.twcert.org.tw/tw/cp-169-10319-38eb7-1.html

Computer and Communications Center
Network Systems Group