POSTING DATE: 2026/01/16

[VULNERABILITY ALERT] SAP Releases Critical Security Advisories for Multiple Products

- Subject: [VULNERABILITY ALERT] SAP Releases Critical Security Advisories for Multiple Products

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202601-00000012
  - [CVE-2026-0501, CVSS: 9.9] This vulnerability exists in SAP S/4HANA Private Cloud and On-Premise (Financials – General Ledger). Due to insufficient input validation, it allows an authenticated attacker to read, modify, and delete backend database data using specially crafted SQL commands.
  - [CVE-2026-0500, CVSS: 9.6] Due to the use of vulnerable third-party components in SAP Wily Introscope Enterprise Manager (WorkStation), an unauthenticated attacker can create a malicious JNLP file accessible via a public URL. When a victim clicks the URL, the Wily Introscope server can execute operating system commands on the victim's computer.
  - [CVE-2026-0498, CVSS: 9.1] This vulnerability exists in SAP S/4HANA Private Cloud and On-Premise. It allows an attacker with administrator privileges to inject arbitrary ABAP code or operating system commands into the system through vulnerabilities in RFC-exposed functional modules, thereby bypassing necessary authorization checks.
  - [CVE-2026-0491, CVSS: 9.1] SAP Landscape Transformation allows an attacker with administrator privileges to exploit vulnerabilities in RFC-exposed functional modules to inject arbitrary ABAP code or operating system commands, bypassing necessary authorization checks.
  - [CVE-2026-0492, CVSS: 8.8] A privilege escalation vulnerability exists in the SAP HANA database. It allows an attacker with valid user credentials to switch to other users, thereby gaining administrator privileges.
- Affected Platforms:
  - SAP S/4HANA Private Cloud and On-Premise (Financials – General Ledger) S4CORE versions 102, 103, 104, 105, 106, 107, 108, 109
  - SAP Wily Introscope Enterprise Manager (WorkStation) WILY_INTRO_ENTERPRISE version 10.8
  - SAP S/4HANA (Private Cloud and On-Premise) S4CORE versions 102, 103, 104, 105, 106, 107, 108, 109
  - SAP Landscape Transformation DMIS versions 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752, 2020
  - SAP HANA database HDB version 2.00
- Recommended Actions:
  - Please refer to the official SAP website for remediation solutions: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2026.html
- Reference Material:

1. https://www.twcert.org.tw/tw/cp-169-10634-69895-1.html

Computer and Communication Center
Network Systems Division, Respectfully