

ANA事件單通知:TACERT-ANA-2026011501014343【漏洞預警】SAP針對旗下多款產品發布重大資安公告

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026011501014343	發佈時間	2026-01-15 13:40:45
事故類型	ANA-漏洞預警	發現時間	2026-01-15 13:40:45
影響等級	低		

[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 資安訊息警訊 TWCERTCC-200-202601-00000012

【CVE-2026-0501，CVSS：9.9】此漏洞存在於SAP S/4HANA私有雲和本地部署(Financials - General Ledger)，由於輸入驗證不足，允許經過身分驗證的攻擊者利用特製的SQL指令進行讀取、修改和刪除後端資料庫資料。

【CVE-2026-0500，CVSS：9.6】由於SAP Wily Introscope Enterprise Manager (WorkStation)使用易受攻擊的第三方元件，未經身分驗證的攻擊者可建立公開URL存取的惡意JNLP文件，導致受害者點擊URL時，Wily Introscope伺服器可在受害者電腦上執行作業系統命令。

【CVE-2026-0498，CVSS：9.1】此漏洞存在於SAP S/4HANA的私有雲和本地部署，允許具有管理員權限的攻擊者透過RFC公開功能模組的漏洞，將任意ABAP程式碼/作業系統命令注入系統，從而繞過必要的授權檢查。

【CVE-2026-0491，CVSS：9.1】SAP Landscape Transformation 允許擁有管理員權限的攻擊者利用RFC公開函數模組漏洞，將任意ABAP程式碼/作業系統命令注入系統，從而繞過必要的授權檢查。

【CVE-2026-0492，CVSS：8.8】SAP HANA 資料庫存在權限提升漏洞，允許攻擊者擁有使用者的有效憑證，即可切換其他用戶，從而獲得管理員權限。

情資分享等級：WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

SAP S/4HANA Private Cloud and On-Premise (Financials - General Ledger) S4CORE 102, 103, 104, 105, 106, 107, 108, 109版本

SAP Wily Introscope Enterprise Manager (WorkStation) WILY_INTRO_ENTERPRISE 10.8版本

SAP S/4HANA (Private Cloud and On-Premise) S4CORE 102, 103, 104, 105, 106, 107, 108, 109版本

SAP Landscape Transformation DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752, 2020版本

SAP HANA database HDB 2.00版本

[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/january-2026.html>

[參考資料:]

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

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw