Boletín de alerta

Boletín Nro.:
Fecha de publicación: 10/12/2025
Tema: Alerta 2025-101 Múltiples Vulnerabilidades Identificadas en Productos SAP
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **SAP Solution Manager** (ST 720)
- **SAP Commerce Cloud** (HY_COM 2205, COM_CLOUD 2211, COM_CLOUD 2211-JDK21)
- **SAP jConnect – SDK for ASE** (16.0.4 y 16.1)
- **SAP Web Dispatcher / Internet Communication Manager (ICM)** (Versiones 7.22 a 9.16)
- **SAP NetWeaver** (módulos BI y servicios remotos, versión 7.50)
- **SAP Business Objects** (Enterprise 430, 2025, 2027)
- **SAP S/4 HANA Private Cloud** (S4CORE 104–109)
- **SAP NetWeaver ICF / SAPUI5 framework** (SAP_BASIS 700–758, SAP_UI 755–758)
- **Application Server ABAP** (kernel 7.53–9.17)
- **SAP Enterprise Search / Enterprise Portal**

Descripción

SAP publicó su boletín de seguridad mensual con 14 vulnerabilidades: 3 críticas, 5 altas y 6 medias, que afectan a múltiples productos de la plataforma SAP. Estas fallas podrían permitir a un atacante ejecutar código malicioso, realizar ataques de deserialización, provocar denegaciones de servicio, acceder a información sensible, explotar SSRF, realizar XSS, omitir autenticación o autorización, manipular memoria y revelar información interna. Debido a la amplia superficie afectada y al impacto potencial sobre la confidencialidad, integridad y disponibilidad de los sistemas, SAP recomienda aplicar los parches oficiales de forma inmediata.

CVE-2025-42880 – Code Injection en SAP Solution Manager (CVSS 9.9)
Una falla por falta de sanitización de entradas permite a un atacante autenticado inyectar código malicioso al invocar un módulo de función remoto, lo que podría otorgarle control total del sistema y comprometer la confidencialidad, integridad y disponibilidad.

CVE-2025-55754 – Vulnerabilidades múltiples en Apache Tomcat dentro de SAP Commerce Cloud (CVSS 9.6)
Tomcat no neutraliza correctamente las secuencias de escape ANSI en los mensajes de registro,

permitiendo que un atacante envíe URLs manipuladas para alterar la consola o portapapeles en sistemas Windows, con intención de engañar a administradores y provocar la ejecución de comandos maliciosos. Varias versiones 9.x, 10.x y 11.x están afectadas y requieren actualización inmediata.

CVE-2025-42928 – Deserialización Insegura en SAP jConnect – SDK for ASE (CVSS 9.1)
Un usuario con privilegios elevados podría aprovechar una entrada especialmente manipulada para desencadenar una deserialización insegura que derive en ejecución remota de código, impactando gravemente la disponibilidad, integridad y confidencialidad del sistema.

Solución:

El fabricante recomienda encarecidamente que el cliente visite el **portal de soporte** y aplique los parches de forma prioritaria para proteger su entorno SAP.

SAP Security Notes & News

Información adicional:

- **https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2025.html**
- **Actualización de seguridad de SAP de diciembre de 2025 | INCIBE-CERT | INCIBE**