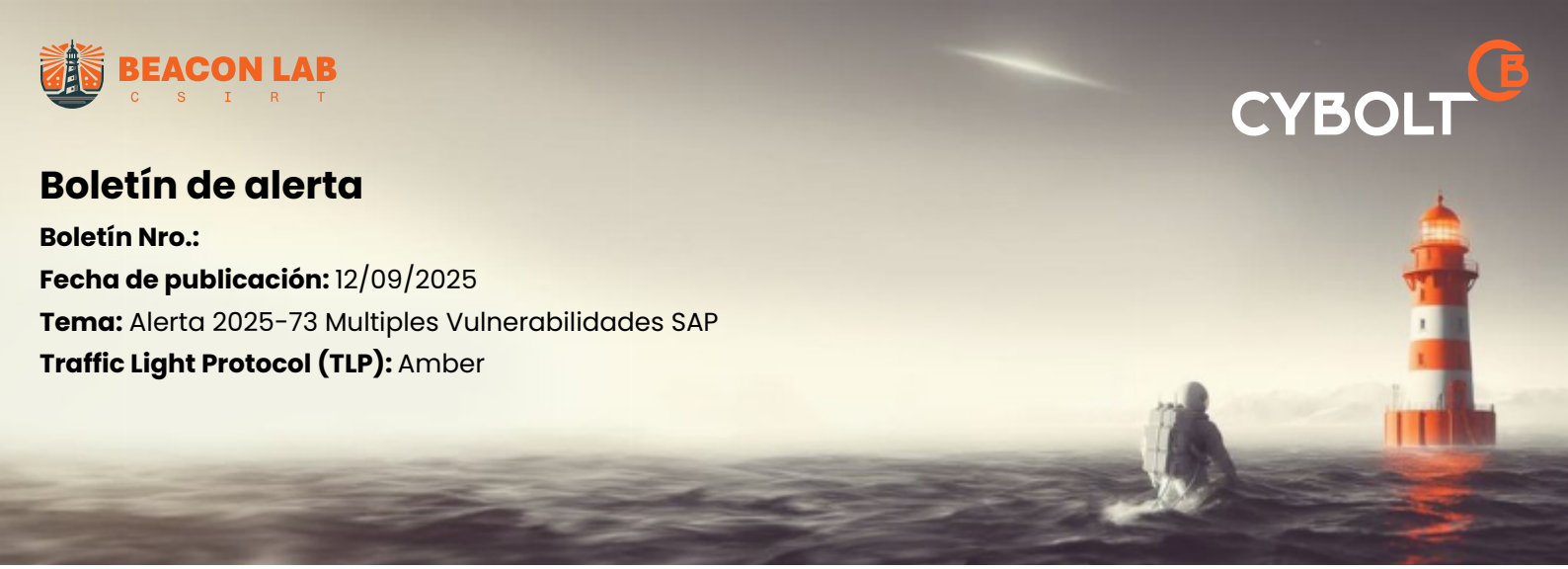

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 12/09/2025
Tema: Alerta 2025-73 Multiples Vulnerabilidades SAP
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- SAP NetWeaver (RMIP4), ServerCore 7.50
- NetWeaver AS Java (Deploy Web Service), J2EE-APPS 7.50

Descripción

SAP ha abordado 21 nuevas vulnerabilidades que afectan a sus productos, incluyendo tres problemas de gravedad crítica que afectan a la solución de software NetWeaver.

SAP NetWeaver es la base de las aplicaciones empresariales de SAP, como ERP, CRM, SRM y SCM, y actúa como un middleware modular ampliamente implementado en grandes redes empresariales.

En su boletín de seguridad de septiembre, el proveedor de software de planificación de recursos empresariales (ERP) menciona una vulnerabilidad con una puntuación de gravedad máxima de 10 sobre 10, identificada como CVE-2025-42944. El problema de seguridad radica en una vulnerabilidad de deserialización insegura en SAP NetWeaver (RMIP4), ServerCore 7.50. Un atacante no autenticado podría explotarla para ejecutar comandos arbitrarios del sistema operativo enviando un objeto Java malicioso a un puerto abierto a través del módulo RMI-P4

RMI-P4 es el protocolo de invocación de métodos remotos (RMI-P4) utilizado por SAP NetWeaver AS Java para la comunicación interna entre SAP o para fines administrativos. Aunque el puerto P4 está abierto en el host, algunas organizaciones podrían exponerlo inadvertidamente a redes más amplias o a Internet debido al firewall u otras configuraciones incorrectas.

La segunda falla crítica corregida por SAP este mes es CVE-2025-42922 (puntuación CVSS v3.1: 9.9), un error de operaciones de archivos inseguros que afecta a NetWeaver AS Java (Implementar servicio web), J2EE-APPS 7.50. Un atacante con acceso autenticado no administrativo puede explotar una falla en la funcionalidad de implementación del servicio web para cargar archivos arbitrarios, lo que podría comprometer por completo el sistema.

La tercera falla es la falta de una comprobación de autenticación en NetWeaver, identificada como CVE-2025-42958 (puntuación CVSS v3.1: 9.1). Esta vulnerabilidad permite que usuarios no autorizados con altos privilegios lean, modifiquen o eliminen datos confidenciales y accedan a funciones administrativas

SAP también abordó las siguientes nuevas vulnerabilidades de alta gravedad:

- CVE-2025-42933 (SAP Business One SLD): Almacenamiento inseguro de datos confidenciales (p. ej., credenciales) que podrían ser extraídos y utilizados de forma indebida.
- CVE-2025-42929 (Servidor de replicación SLT): Falta de validación de entrada, lo que permite que entradas maliciosas corrompan o manipulen datos replicados.
- CVE-2025-42916 (S/4HANA): Falta de validación de entrada en componentes principales, lo que supone un riesgo de manipulación no autorizada de datos

Mitigación:

Se recomienda a los administradores de sistemas que sigan las recomendaciones de parcheo y mitigación para las tres fallas críticas, disponibles para los clientes con una cuenta SAP.

- https://me.sap.com/notes/3634501
- https://me.sap.com/notes/3643865
- https://me.sap.com/notes/3627373

Información adicional:

- https://cyberpress.org/sap-releases-security-updates/
- https://www.bleepingcomputer.com/news/security/sap-fixes-maximum-severity-netweaver-command-execution-flaw/
- https://securityonline.info/sap-security-patch-day-fixes-four-critical-flaws-including-a-cvss-10-0-rce-cve-2025-42944/