Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD CRÍTICA EN SAP S4HANA (CVE-2025-42957) BAJO EXPLOTACIÓN ACTIVA

05/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

La ciberseguridad empresarial enfrenta un nuevo desafío con la revelación de una vulnerabilidad crítica en SAP S/4HANA, una de las soluciones de planificación de recursos empresariales (ERP) más utilizadas en el mundo. El fallo, identificado como CVE-2025-42957, ha sido clasificado con un CVSS de 9.9, lo que refleja su nivel de riesgo extremo. Lo más preocupante es que ya se encuentra bajo explotación activa en entornos reales, poniendo en jaque a organizaciones que dependen de SAP para la operación de procesos estratégicos.

Este tipo de vulnerabilidades no solo amenazan la integridad técnica de los sistemas, sino también la continuidad de negocio y la protección de datos críticos. La explotación de CVE-2025-42957 puede permitir a un atacante comprometer de manera total un entorno SAP, abriendo la puerta a fraudes financieros, espionaje corporativo o incluso la instalación de ransomware. Ante este panorama, la aplicación inmediata de medidas de mitigación es esencial para reducir riesgos y fortalecer la resiliencia empresarial.

VULNERABILIDAD CRÍTICA EN SAP S4HANA (CVE-2025-42957) BAJO EXPLOTACIÓN ACTIVA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_05_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/09/2025
Es día cero (0 day):	No

RESUMEN

Un riesgo elevado para entornos ERP

SAP S/4HANA, una de las plataformas de planificación de recursos empresariales (ERP) más utilizadas a nivel mundial, se ve afectada por una vulnerabilidad crítica que ya está siendo explotada en escenarios reales. El fallo, identificado como CVE-2025-42957 y con una puntuación CVSS de 9.9, fue corregido en las actualizaciones de seguridad mensuales de SAP el mes pasado.

Inyección de código y escalada de privilegios

La vulnerabilidad permite a un atacante con credenciales de bajo nivel aprovechar un módulo RFC para inyectar código ABAP arbitrario. Esto significa que puede burlar controles de autorización, comprometiendo la confidencialidad, integridad y disponibilidad del sistema. Entre los posibles impactos se encuentran:

- Creación de usuarios con privilegios de superadministrador (SAP_ALL).
- Alteración de la base de datos.
- Descarga de hashes de contraseñas.
- Manipulación de procesos de negocio críticos.

En términos prácticos, el defecto abre la puerta a fraude, robo de datos, espionaje corporativo o incluso la instalación de ransomware en entornos SAP.

Impacto en on-premise y nube privada

De acuerdo con investigadores, la vulnerabilidad afecta tanto a implementaciones on-premise como en Private Cloud. El proceso de explotación es relativamente sencillo y no requiere privilegios elevados, lo que incrementa el riesgo de que actores maliciosos busquen aprovecharlo de forma masiva en el corto plazo.

Recomendaciones de seguridad

Aunque aún no se han detectado campañas de explotación generalizada, los expertos advierten que revertir el parche y crear un exploit resulta fácil para los atacantes. Por ello, se recomienda a las organizaciones que utilizan SAP S/4HANA:

1. Aplicar de inmediato los parches de SAP.
2. Monitorear registros de actividad, especialmente llamadas RFC sospechosas o la creación de nuevos usuarios con privilegios elevados.
3. Revisar la segmentación de red para limitar el alcance de un posible ataque.
4. Mantener copias de seguridad actualizadas y listas para una restauración rápida.
5. Implementar SAP UCON para restringir el uso de RFC.
6. Revisar y limitar accesos al objeto de autorización S_DMIS (actividad 02).

Conclusión

La vulnerabilidad CVE-2025-42957 representa un riesgo crítico para las organizaciones que dependen de SAP S/4HANA para gestionar procesos empresariales clave. La explotación ya ha sido confirmada en la naturaleza, lo que convierte la aplicación inmediata de medidas de seguridad en una prioridad estratégica para evitar consecuencias de gran impacto.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-critica-en-sap-s-4hana-cve-2025-42957-bajo-explotacion-activa/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/