Boletín de alerta

Boletín Nro.:
Fecha de publicación: 20/08/2025
Tema: Alerta 2025-71 Explotacion activa de vulnerabilidades de SAP
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- SAP Netweaver 7.50
- SAP Netweaver 7.5

Descripción

Se han identificado dos fallas críticas en SAP NetWeaver Visual Composer que, aunque ya cuentan con parches oficiales, actualmente están siendo explotadas de manera activa por diferentes actores de amenazas.

La primera vulnerabilidad, registrada como **CVE-2025-31324** y con una puntuación CVSS de 10.0, corresponde a una falta de comprobación de autorización. Esta falla permite que un atacante no autenticado pueda subir archivos maliciosos directamente al servidor afectado, lo que abre la puerta a un compromiso total del sistema SAP, afectando su confidencialidad, integridad y disponibilidad.

La segunda vulnerabilidad, identificada como **CVE-2025-42999** y con una puntuación CVSS de 9.1, está relacionada con un proceso de **deserialización insegura**. En este caso, un usuario privilegiado puede cargar contenido malicioso que, al ser procesado, se ejecuta con permisos elevados. Esto permite a los atacantes tomar control del sistema, ejecutar código remoto y comprometer tanto los datos como los procesos críticos de negocio.

Actualmente, estas vulnerabilidades en conjunto no son meramente teóricas; están siendo **explotadas de manera activa en ataques reales y dirigidos** contra organizaciones.

- **Ransomware en expansión**

Grupos como **Qilin, BianLian y RansomEXX** han incorporado estas fallas en sus campañas. Su objetivo principal es **interrumpir operaciones empresariales**, **cifrar datos críticos** y **extorsionar a las organizaciones** a cambio de un rescate.
Estos grupos son conocidos por actuar de manera rápida y oportunista: tan pronto como surge una nueva

vulnerabilidad crítica, la integran en sus ataques para maximizar el impacto antes de que las empresas apliquen los parches.

- **Campañas de espionaje**

Además de las operaciones de ransomware, se ha identificado el uso de estas vulnerabilidades por **actores de amenazas vinculados a China**, enfocados en **infraestructura crítica y redes corporativas estratégicas**. En este contexto, el objetivo no es necesariamente económico, sino el **robo de información sensible** para fines de espionaje industrial.

- **Tácticas avanzadas de ataque**

El exploit permite no solo la instalación de webshells para mantener acceso remoto, sino también el uso de técnicas "Living off the Land" (LotL). Esto significa que los atacantes pueden ejecutar comandos directamente en el sistema operativo usando herramientas legítimas de SAP o del propio sistema, reduciendo la probabilidad de ser detectados por soluciones de seguridad tradicionales.

Solución:

Actualizar inmediatamente los dispositivos a la version **mas actual**

Información adicional:

- https://thehackernews.com/2025/08/public-exploit-for-chained-sap-flaws.html
- https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

  https://accounts.sap.com/saml2/idp/sso