LUMA

BOLETÍN DE SEGURIDAD CIBERNÉTICA

27 de Abril, 2025

TLP: CLEAR

Vulnerabilidad SAP VISUAL NETWEAVER7 CVE-2025-313324

Impacto:
Alto – 10

CVE:
CVE-2025-31324

Descripción:

SAP y Onapsis han publicado una nota de seguridad para comunicar la existencia de una vulnerabilidad 0 day de severidad critica que podría permitir a un atacante, no autenticado, explotar la vulnerabilidad para obtener el control total de los sistemas SAP.Se tiene constancia de que dicha vulnerabilidad esta siendo explotada de forma activa mediante ransomware

Detalles técnicos de la Vulnerabilidad:

Una vulnerabilidad crítica ha sido identificada en SAP NetWeaver Visual Composer (CVE-2025-31324), con un puntaje CVSS v3 de 10.0, lo que indica la gravedad de la falla. La vulnerabilidad afecta al componente Metadata Uploader de SAP NetWeaver Visual Composer y permite a los atacantes cargar archivos maliciosos de manera no autenticada.
La vulnerabilidad en cuestión es de carga de archivos no autenticados, lo que significa que un atacante no necesita iniciar sesión para explotar la vulnerabilidad. Este fallo permite a los atacantes cargar archivos ejecutables maliciosos en el sistema, lo que puede dar lugar a la ejecución remota de código (RCE). En consecuencia, un atacante podría obtener control total sobre el sistema afectado, comprometiendo así toda la infraestructura relacionada.
Si un atacante aprovecha con éxito esta vulnerabilidad, podría ejecutar código malicioso en el sistema vulnerable sin la necesidad de autenticación previa. Esto podría llevar al compromiso completo de los sistemas SAP afectados, alterando la integridad de los datos, interrumpiendo los servicios e incluso permitiendo la escalada de privilegios.

CÓMO SE EXPLOTA (ESCENARIO DE ATAQUE)

La vulnerabilidad reside en la /developmentserver/metadatauploader punto final de Visual Composer de SAP NetWeaver. Debido a la falta de comprobaciones de autorización, Los atacantes pueden cargar archivos JSP maliciosos sin autenticación. Una vez cargado en el servlet_jsp/irj/root/ directorio, Estos archivos se pueden ejecutar de forma remota, otorgar a los atacantes control sobre el sistema.

Se descubrió que los atacantes están aprovechando esto Vulnerabilidad de SAP para implementar shells web JSP, Facilitar la carga no autorizada de archivos y la ejecución de código. Técnicas avanzadas, Incluyendo el uso de Brute Ratel y el método Heaven's Gate, Se ha observado que mantienen la persistencia y evaden la detección.. En algunos casos, Los atacantes han tardado días en pasar del acceso inicial a una mayor explotación., Sugiriendo la participación de intermediarios de acceso inicial.

RECURSOS AFECTADOS

- **SAP NetWeaver Application Server:** Si está habilitado el Visual Composer, este componente queda expuesto a la vulnerabilidad.
- **SAP Business Suite:** Dado que SAP NetWeaver es la base de otras aplicaciones de SAP, como SAP ERP, SAP CRM y SAP BW, los sistemas que dependan de SAP NetWeaver pueden estar comprometidos.
- **Plataformas de integración y desarrollo de SAP:** La vulnerabilidad podría afectar la integridad de aplicaciones personalizadas y procesos de integración entre sistemas de SAP y otras plataformas externas.

MEDIDAS DE MITIGACIÓN RECOMENDADAS

SAP ha publicado actualizaciones para abordar esta vulnerabilidad crítica. Es esencial aplicar los parches lo más rápido posible para proteger los sistemas afectados.

- Visita el portal de soporte de SAP: En el portal de soporte de SAP (SAP ONE Support Launchpad), puedes acceder a los parches y correcciones más recientes

para la vulnerabilidad.

- Parche específico para Visual Composer: Asegúrate de aplicar el parche que corrige específicamente el componente Metadata Uploader.
- Proceso de actualización: Dependiendo de la versión de SAP NetWeaver que utilices, el proceso para aplicar el parche puede variar. Consulta la guía de instalación de SAP para instrucciones detalladas.
- Limitar el acceso a la ruta **/developmentserver** punti final a través de reglas de firewall
- Inspeccionar regularmente el **servlet_jsp/irj/root/** directorio para archivos no autorizados
- Si el componente Visual Composer no esta en uso, considere deshabilitar el componente visual para reducir las superficies de ataque.

ACCIONES RECOMENDADAS

Se recomienda aplicar las actualizaciones de seguridad proporcionadas por SAP para mitigar esta vulnerabilidad. Los parches están disponibles en el portal de soporte de SAP.
Monitoreo de logs: Es importante realizar un monitoreo constante de los logs del sistema para detectar cualquier actividad inusual que pueda estar relacionada con intentos de explotación de esta vulnerabilidad.
Restricciones de acceso: Limitar el acceso al componente afectado (Metadata Uploader) y revisar las configuraciones de seguridad de SAP NetWeaver para reducir la superficie de ataque.
Si se ve alguna actividad sospechosa con relación con SAP se recomienda realizar una auditoría de seguridad para verificar la integridad de los sistemas y la ausencia de posibles accesos no autorizados.

REFERENCIAS Y ENLACES OFICIALES

- https://community.sap.com/
- https://nvd.nist.gov/vuln/detail/CVE-2025-31324
- https://www.bleepingcomputer.com/news/security/sap-fixes-suspected-netweaver-zero-day-exploited-in-attacks/
- https://blog.segu-info.com.ar/2025/04/zero-day-critico-en-sap-netweaver-7xx.html?m=1