Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD ZERO-DAY EN SAP VISUAL COMPOSER CVE-2025-31324

26/ 04 / 2025

CONTENIDO

INTRODUCCIÓN

En los últimos días, el mundo de la ciberseguridad empresarial ha encendido las alertas ante la aparición de una nueva vulnerabilidad crítica que afecta a sistemas SAP: el CVE-2025-31324. Esta vulnerabilidad, calificada con la máxima severidad (CVSS 10.0), permite a atacantes no autenticados comprometer totalmente sistemas SAP que utilizan el componente Visual Composer. Detectada gracias a reportes de múltiples firmas de respuesta a incidentes y confirmada por SAP, su explotación activa en entornos expuestos a Internet plantea riesgos serios para la continuidad de negocio y la integridad de datos críticos. El fallo reside en la falta de validaciones de autenticación y autorización en un módulo clave, permitiendo la carga de archivos maliciosos como webshells. Afortunadamente, SAP ha emitido parches de emergencia y medidas de mitigación para contener el riesgo. En este artículo te explicamos en detalle qué implica esta amenaza, cómo detectar si tu empresa está en riesgo y las acciones recomendadas para proteger tus sistemas SAP.

VULNERABILIDAD ZERO-DAY EN SAP VISUAL COMPOSER CVE-2025-31324

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

ID de alerta:	DSOC-CERT_2025_04_26_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	26/04/2025
Es día cero (0 day):	No

RESUMEN

Una vulnerabilidad crítica (CVE-2025-31324) en SAP Visual Composer, parte del entorno SAP NetWeaver Java, ha sido detectada y se encuentra actualmente siendo explotada en entornos reales. Esta falla, catalogada con un nivel de severidad crítica (CVSS 10.0), permite que actores maliciosos no autenticados comprometan completamente los sistemas SAP afectados.

¿Qué está ocurriendo?

SAP Visual Composer, aunque no instalado por defecto, está presente en un gran número de sistemas debido a su utilidad para usuarios de negocio que desarrollan aplicaciones sin necesidad de programación. El problema detectado radica en una falta de controles adecuados de autenticación y autorización en su módulo “developmentserver”, permitiendo la carga arbitraria de archivos maliciosos a través de solicitudes HTTP/HTTPS.

El ataque en acción

Investigadores y diversas firmas de respuesta a incidentes han observado actividad maliciosa dirigida a esta vulnerabilidad. El método de ataque es relativamente simple: mediante una solicitud POST cuidadosamente elaborada al componente vulnerable (/developmentserver/metadatauploader), los atacantes pueden cargar webshells como helper.jsp o cache.jsp, otorgándoles control completo del sistema con los privilegios del xusuario operativo <sid>adm.

Los riesgos derivados son enormes: desde la alteración de datos financieros y el acceso a información confidencial, hasta la instalación de ransomware o la interrupción completa de operaciones críticas de negocio.

¿A quiénes afecta?

Todos los sistemas SAP NetWeaver Java 7.xx, en cualquier versión de soporte (SPS), son vulnerables si tienen instalado el componente “Visual Composer Framework” o “VCFRAMEWORK”. Incluso si su sistema no está expuesto directamente a Internet, esta vulnerabilidad puede ser aprovechada por amenazas internas o malware que ya haya penetrado la red corporativa.

Cómo identificar la vulnerabilidad

Para verificar si su sistema es vulnerable:

Acceda a System Information en su servidor SAP NetWeaver Java.

Revise el listado de componentes instalados.

Si encuentra “VISUAL COMPOSER FRAMEWORK” o “VCFRAMEWORK”, su sistema requiere atención inmediata.

¿Qué hacer ahora?

SAP ha emitido un parche de emergencia en la nota de seguridad SAP 3594142. También se han dispuesto medidas de mitigación en la nota SAP 3593336 para aquellos que no puedan aplicar el parche de inmediato.

Además, SAP ha proporcionado una guía para identificar signos de compromiso en los sistemas, incluyendo la búsqueda de archivos .jsp, .java o .class en rutas específicas del sistema de archivos SAP.

Indicadores de compromiso (IoCs) conocidos:

Webshell helper.jsp: Hash SHA256
1f72bd2643995fab4ecf7150b6367fa1b3fab17afd2abed30a98f075e4913087

Webshell cache.jsp: Hash SHA256
794cb0a92f51e1387a6b316b8b5ff83d33a51ecf9bf7cc8e88a619ecb64f1dcf

Impacto

El compromiso de un servidor SAP puede tener consecuencias devastadoras: alteración de operaciones críticas, filtración de datos sensibles, incumplimiento de regulaciones como la NIS2 en Europa o las normas de ciberseguridad de la SEC en EE.UU., además de daños irreparables a la reputación empresarial.

Recomendaciones

Actúe de inmediato:

Aplique el parche de SAP o implemente las medidas de mitigación.

Realice una evaluación exhaustiva de sus sistemas SAP.

Si sospecha de un compromiso, active su plan de respuesta a incidentes sin demora.

La amenaza es real, el tiempo es crítico, y proteger los sistemas SAP de su empresa nunca ha sido más importante.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-zero-day-en-sap-visual-composer-cve-2025-31324/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@develsecurity.com

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://www.devel.group/