Nro. Alerta:	AL-2025-022	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	26-may-2025	Vulnerabilidad de SAP VC (CVE-2025-31324)	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Falla crítica en SAP
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad de SAP VC - figura referencial

CVE-2025-31324: Una falla crítica en SAP NetWeaver Visual Composer (VC) que permite la ejecución remota de código sin autenticación que ya ha sido explotada por grupos de Ransomware como Qilin, BianLian y RansomExx.

III. INTRODUCCIÓN

SAP VC, es la herramienta de modelado de software basada en la web, produce aplicaciones en forma declarativa, es decir, en diseño visual de interfaces (arrastrar y soltar) para aplicaciones y dashboards, permitiendo ejecutarlas sin la creación de código para múltiples entornos en tiempo de ejecución, debido a su arquitectura abierta permite a los desarrolladores ampliar su entorno de tiempo de diseño y su lenguaje moderado, así como para integrar servicios de datos de fuentes externas, como del Data Warehouse corporativo de SAP Business Warehouse (BW).

SAP BW usa la herramienta Metadata Uploader que permite cargar metadatos de forma masiva mediante archivos estructurados (como Excel o CSV), eliminando la necesidad de crear objetos manualmente en el sistema, esta utilidad integra:

- Automatizar la creación/modificación de objetos técnicos (InfoObjects, Cubos, DSOs, etc.).
- Ahorra tiempo en implementaciones o migraciones donde se requieren muchos objetos.
- Valida la estructura de los datos antes de la carga.

La vulnerabilidad CVE-2025-31324 reside en este componente de Metadata Uploader de SAP VC, el cual no controla adecuadamente la autenticación y autorización, permitiendo a atacantes no autorizados subir archivos maliciosos como wbshells JPS, a través del endpoint /developmentserver/metadatauploader, resultando en la ejecución remota de código.

Se ha confirmado que esta vulnerabilidad fue explotada activamente por atacantes del grupo de Ransomware Qilin para desplegar herramientas de acceso remoto y Ransomware en demás entornos empresariales.

IV. VECTOR DE ATAQUE

El ataque se lleva a cabo de manera remota y es del tipo red.

CVSS:3.1/AV:**N**/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H de puntuación Alta 10.

Debido a que SAC VC Metadata Uploader no está protegido con una autorización adecuada, permite a un atacante no autenticado cargar binarios ejecutables maliciosos con lo que afectaría gravemente al sistema host, la confidencialidad, integración y disponibilidad del sistema objetivo.

1. **Fase inicial**

   El ataque comienza enviando solicitudes POST diseñadas para un dispositivo final vulnerable, cargando web shells JSP como helper.jsp, cache.jsp o cualquier archivo con extensiones. jsp, alojándose en directorios accesibles públicamente, como j2ee/cluster/apps/sap.com/irj/servlet_jsp/irj/root/, una vez cargado permite la ejecución remota de comandos con privilegios administrativos.

2. Recopilación de información

Establecido el acceso, el atacante realiza el reconocimiento del sistema utilizando comandos para obtener información del sistema y su entorno de red:

- cat /etc/hosts
- ps –ef
- netstat –tenp
- uname -a

3. Persistencia

Para mantener su persistencia y facilitar la explotación más profunda se usa algunas herramientas:

- **GOREVERSE**: Herramienta de shell inverso que permite acceso remoto y transferencias de archivos.

- **Brute Ratel y Heaven's Gate**: Utilizadas para comunicación de comando, control y técnicas de evasión.

- **XMRig Miner:** Se despliega para secuestrar recursos del sistema para minería de criptomonedas.

V. IMPACTO

La vulnerabilidad afecta a los productos SAP NetWeaver v7.50 y 7.40.

VI. INDICADORES DE COMPROMISO

- Intentos de acceso no autorizado a la ruta /developmentserver/metadatauploader.
- Cargar archivos JSP inesperados en el directorio servlet_jsp/irj/root/, tales como helper.jsp y cache.jsp.
- Conexiones salientes no autorizadas desde sus sistemas SAP.
- Verifique la ruta de los siguientes directorios del sistema operativo para detectar la presencia de archivos 'jsp', 'java' o 'class'.
- C:\usr\sap\<SID>\<InstanceID>\j2ee\cluster\apps\sap.com\irj\servlet_jsp\irj\root.

- C:\usr\sap\<SID>\<InstanceID>\j2ee\cluster\apps\sap.com\irj\servlet_jsp\irj\work.
- C:\usr\sap\<SID>\<InstanceID>\j2ee\cluster\apps\sap.com\irj\servlet_jsp\irj\work\sync.

VII. RECOMENDACIONES

- Aplicar el parche oficial publicado por SAP mediante la nota de seguridad #3594142, emitida el 24 de abril de 2025.
- Deshabilitar el componente Visual Composer si no se utiliza, para reducir la superficie de ataque.
- Restringir el acceso al endpoint vulnerable /developmentserver/metadatauploader utilizando reglas de firewall o controles de acceso adecuados.
- Monitorear los directorios mencionados para identificar archivos JSP no autorizados y revisar los logs del sistema en busca de actividad sospechosa.
- Utilizar herramientas de análisis de indicadores de compromiso, como el escáner desarrollado por Onapsis y Mandiant, para verificar posibles intrusiones.
- Actualizar SAP NetWeaver a las versiones corregidas:
- 7.50: Aplicar Support Packages SP027 a SP033.
- 7.40 y anteriores: Implementar medidas de mitigación alternativas debido a la falta de soporte.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Onapsis (2025). SAP NetWeaver Flaw Lets Threat Actors Take Full Control: CVE-2025-31324 and CVE-2025-42999 Explained. https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/

Vahagn Vardanian (2025). RedRAYS. [CVE-2025-31324] Critical SAP NetWeaver Vulnerability Fixed: Actively Exploited in the Wild. https://redrays.io/blog/critical-sap-netweaver-vulnerability-cve-2025-31324-fixed-actively-exploited-in-the-wild/

Incibe (2025). Vulnerabilidad en SAP NetWeaver Visual Composer Metadata Uploader (CVE-2025-31324). https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2025-31324

NIST (2025). CVE-2025-31324 Detail. https://nvd.nist.gov/vuln/detail/CVE-2025-31324

CVE (2025). CVE-2025-31324. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-31324

Sensors (2025). Falla crítica de SAP NetWeaver (CVE-2025-31324) Explotado activamente. https://sensorstechforum.com/es/cve-2025-31324-actively-exploited/