Nro. Alerta:	AL-2025-010	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	12-mar-2025	Vulnerabilidad en Python-Json-Logger- CVE-2025-27607	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Nivel de riesgo: Alta

II. ALERTA

CVE-2025-27607 es una vulnerabilidad de la biblioteca Python-Json-Logger v3.2.x de Python v3.13.

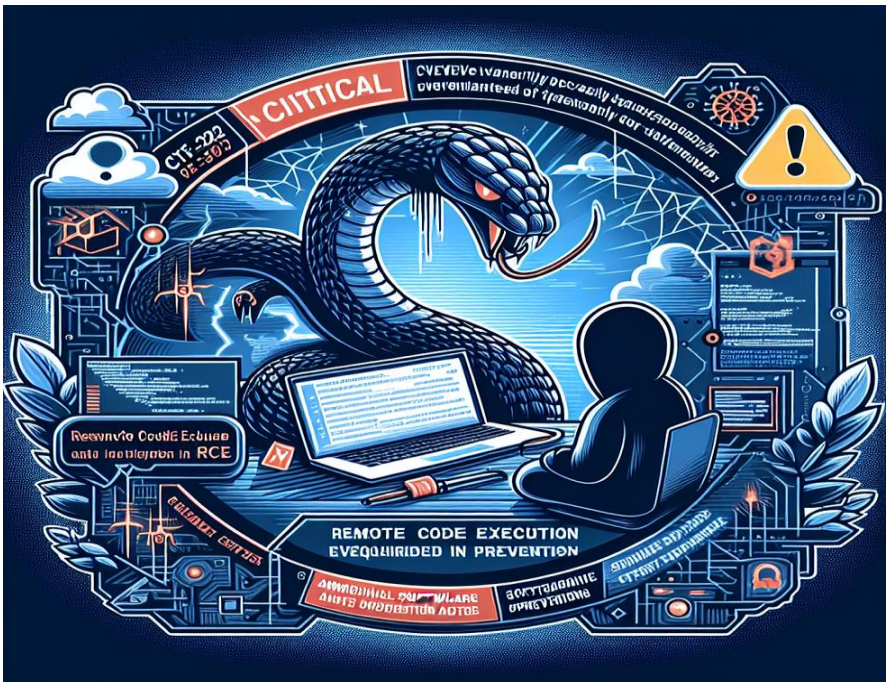


Figura 1.- *Vulnerabilidad en Python-Json-Logger* - figura referencial

La biblioteca Python-Json-Logger es ampliamente utilizada para la generación de logs en formato JSON y cuenta con una gran popularidad, alcanzando más de 43 millones de descargas mensuales. Debido a su amplio uso, la explotación de esta vulnerabilidad CVE-2025-27607 representa un riesgo crítico, ya que permite la ejecución remota de código (RCE) en sistemas vulnerables.

III. INTRODUCCIÓN

Python-Json-Logger es una herramienta utilizada por desarrolladores para registrar logs en formato JSON, que facilita el análisis y manejo de registros en aplicaciones de Python. El formato JSON es utilizado para el intercambio de datos entre sistemas, pero una mala

implementación o una vulnerabilidad en el manejo de estos datos pueden ser explotadas para comprometer un sistema.

La vulnerabilidad surge debido a una dependencia opcional eliminada msgspec-python313-pre en el archivo pyproject.toml. Al ser este paquete borrado de PyPI (Official third-party software repository for Python) deja su nombre libre y sin reclamar. Por lo que un atacante podría publicar un paquete malicioso bajo el mismo nombre msgspec-python313-pre que al ser instalado automáticamente en entornos de Python 3.13 ejecuta código arbitrario. Esta vulnerabilidad está clasificada bajo CWE-829 Inclusion of Functionality from Untrusted Control Sphere, que es un problema de seguridad que ocurre cuando un software incorpora código, bibliotecas o funcionalidades provenientes de fuentes externas que no son completamente confiables o controladas, permitiendo introducir vulnerabilidades en el sistema, ya que los componentes no confiables pueden contener código malicioso, errores o comportamientos no deseados que podrían ser explotados por el atacante.

La vulnerabilidad está asociada con la deserialización insegura de datos en Python-Json-Logger. Cuando los objetos JSON se deserializan de forma incorrecta, los datos maliciosos pueden ser interpretados como código Python, lo que abre la posibilidad a la ejecución remota de código (RCE) esto ocurre si se procesa un archivo JSON malintencionado.

IV. VECTOR DE ATAQUE

Puntuación: 8.8 - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Para demostrar cómo funciona este ataque, analicemos el proceso de explotación:
El atacante obtiene ejecución remota de código en el sistema del desarrollador o CI/CD.

1. **Identificar una dependencia faltante:**

   - Los atacantes escanean paquetes populares en busca de dependencias que no existen en PyPI.
   - Usando herramientas como pipreqs, pueden enumerar dependencias y verificar si falta alguna.

2. **Registrar un paquete con código malicioso:**

   - El atacante se registra msgspec-python313-pre en PyPI.
   - Dentro de este paquete, incluyen un setup.py script malicioso.

- Alternativamente, podrían incrustar el payload en el interior __init__.py para que se ejecute al importarla.

3. **Espere a que las víctimas instalen la dependencia:**

- Cualquier usuario que ejecute pip install python-json-logger[dev] con Python 3.13 instalaría automáticamente el paquete malicioso.
- El atacante obtiene ejecución remota de código en el sistema del desarrollador o CI/CD.

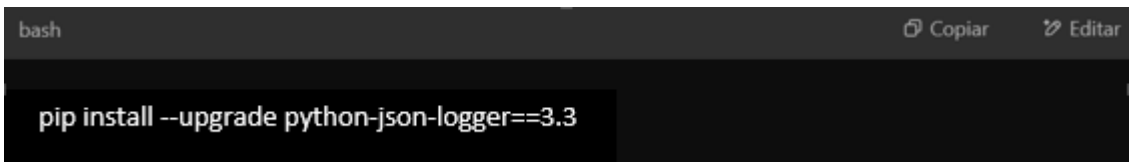
V. IMPACTO

Según los datos de PyPI BigQuery, python-json-logger recibe más de 46 millones de descargas mensuales. Esto implica que incluso una pequeña fracción de usuarios que instalen las dependencias de desarrollo podría generar una vulneración masiva, afectando a una gran cantidad de sistemas. Dicha vulnerabilidad yace en entornos Python 3.13.x con instalación de la biblioteca python-json-logger[dev] en las versiones vulnerables 3.2.0 y 3.2.1.

Para las organizaciones que dependen de entornos de integración continua y despliegue continuo (CI/CD), donde las dependencias se instalan de forma automatizada y dinámica, esta vulnerabilidad representa un riesgo significativo. Podría desencadenar un ataque a la cadena de suministro de software, comprometiendo no solo los entornos de desarrollo, sino también sistemas sensibles. Esto abre la puerta a una serie de amenazas, como la exfiltración de credenciales, claves de API y datos confidenciales, así como la posibilidad de implementar malware a gran escala, lo que afectaría tanto a la infraestructura interna de la organización como a los usuarios finales.

VI. RECOMENDACIONES

- Se recomienda actualizar a la última versión 3.3 de esta dependencia python-json-logger para corregir la vulnerabilidad, mediante el siguiente comando:



- Verificar el changelog oficial del paquete para asegurarse de que la versión utilizada no está afectada.

- Implementar herramientas como pip-audit para escanear vulnerabilidades en dependencias:

```bash
pip install pip-audit
pip-audit
```

- Utilizar requirements.txt o poetry.lock para gestionar versiones específicas de los paquetes y evitar actualizaciones automáticas no supervisadas.
- Ejecutar procesos en entornos restringidos para evitar que una vulnerabilidad en python-json-logger tenga acceso a recursos críticos del sistema.
- Configurar permisos adecuados para los archivos de logs generados.
- Filtrar y validar los datos de entrada antes de incluirlos en los logs para evitar inyección de código malicioso.
- Utilizar herramientas como pysec o bandit para analizar código en busca de posibles fallos de seguridad.
- Configurar herramientas de monitoreo como SIEM (Security Information and Event Management) para detectar patrones de explotación.
- Implementar registros de auditoría y alertas para detectar intentos de explotación de la vulnerabilidad.

VII. 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.

VIII. REFERENCIAS:

https://nvd.nist.gov/vuln/detail/CVE-2025-27607

https://www.piwheels.org/project/python-json-logger/

https://www.upwind.io/feed/supply-chain-remote-code-execution-in-python-json-logger-cve-2025-27607

Nro. Alerta:	AL-2025-010	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	12-mar-2025	Vulnerabilidad en Python-Json-Logger- CVE-2025-27607	Pág.: **5** of **5**

https://github.com/nhairs/python-json-logger/security/advisories/GHSA-wmxh-pxcx-9w24

https://vuldb.com/?id.298960

https://secalerts.co/vulnerability/CVE-2025-27607

https://feedly.com/cve/CVE-2025-27607

https://www.rescana.com/post/critical-cve-2025-27607-vulnerability-in-python-json-logger-update-to-prevent-remote-code-execution