Se ha revelado una vulnerabilidad crítica de seguridad en el Kit de Desarrollo de Software (SDK) de Apache Avro Java que, si se explota con éxito, podría permitir la ejecución de código arbitrario en instancias vulnerables.

La falla, rastreada como CVE-2024-47561, afecta a todas las versiones del software anteriores a la 1.11.4.

> *"El análisis de esquemas en el SDK de Java de Apache Avro 1.11.3 y versiones anteriores permite a actores maliciosos ejecutar código arbitrario. Se recomienda a los usuarios actualizar a la versión 1.11.4 o 1.12.0, que corrige este problema»,* dijeron los mantenedores del proyecto en un aviso publicado la semana pasada.

Apache Avro, análogo a Protocol Buffers (protobuf) de Google, es un proyecto de código abierto que proporciona un marco de serialización de datos neutral en cuanto al lenguaje, diseñado para el procesamiento de datos a gran escala.

El equipo de Avro señala que la vulnerabilidad afecta a cualquier aplicación que permita a los usuarios proporcionar sus propios esquemas Avro para su análisis. Kostya Kortchinsky, del equipo de seguridad de Databricks, ha sido acreditado con el descubrimiento y la denuncia de esta deficiencia de seguridad.

Como medidas de mitigación, se recomienda sanitizar los esquemas antes de analizarlos y evitar analizar esquemas proporcionados por usuarios.

> *"CVE-2024-47561 afecta a Apache Avro 1.11.3 y versiones anteriores al deserializar entradas recibidas a través del esquema avroAvro"*, dijo Mayuresh Dani, gerente de investigación de amenazas en Qualys.
>
> *"El procesamiento de dicha entrada por parte de un actor de amenazas conduce a*

> *la ejecución de código. Según nuestros informes de inteligencia de amenazas, no hay una prueba de concepto (PoC) disponible públicamente, pero esta vulnerabilidad existe al procesar paquetes a través de las directivas ReflectData y SpecificData y también puede ser explotada a través de Kafka».*
>
> *«Dado que Apache Avro es un proyecto de código abierto, es utilizado por muchas organizaciones. Según los datos disponibles públicamente, la mayoría de estas organizaciones se encuentran en los EE. UU. Esto tiene muchas implicaciones de seguridad si no se corrige, supervisa y protege».*