Investigadores de seguridad cibernética descubrieron el lunes configuraciones incorrectas en versiones anteriores de instancias de Apache Airflow, que pertenecen a una serie de empresas de alto perfil en varios sectores, lo que resultó en la exposición de credenciales confidenciales para plataformas y servicios populares como Amazon Web Services (AWS), Binance, Google Cloud Platform (GCP), PayPal, Slack y Stripe.

> *«Estas instancias no seguras exponen información confidencial de empresas en las industrias de medios, finanzas, manufactura, tecnología de la información (TI), biotecnología, comercio electrónico, salud, energía, seguridad cibernética y transporte»,* dijo Intezer en un informe.

Lanzado originalmente en junio de 2015, Apache Airflow es una plataforma de administración de flujo de trabajo de código abierto que permite la programación y el monitoreo programáticos de los flujos de trabajo en AWS, GCP, Microsoft Azure y otros servicios de terceros. También es una de las herramientas de orquestación de tareas más populares, seguida de Luigui, Kubeflow y MLflow.

Algunas de las prácticas de codificación inseguras más comunes descubiertas por Intezer incluyen el uso de contraseñas de bases de datos codificadas en código o variables de Python DAG, credenciales de texto sin formato en el campo de conexiones «Extra» y claves de texto sin formato en archivos de configuración (airflow.cfg).

La principal de las preocupaciones asociadas con las instancias de Airflow mal configuradas es la exposición de credenciales, que podrían ser abusadas por los hackers para obtener acceso a cuentas y bases de datos, lo que les brinda la capacidad de propagarse lateralmente o resultar en una fuga de datos, sin mencionar que conducen a una violación de datos y dan una idea de las herramientas y paquetes de una organización, que luego podrían explotarse para organizar ataques a la cadena de suministro.

> *«Si hay una gran cantidad de contraseñas visibles, un actor de amenazas también*

> *puede usar estos datos para detectar patrones y palabras comunes para inferir otras contraseñas. Estos se pueden aprovechar en ataques de diccionario o de estilo de fuerza bruta contra otras plataformas»,* dijeron los investigadores.

Más preocupante que esto, es la posibilidad de que se pueda lanzar malware en los entornos de producción expuestos al aprovechar la función Variables para modificar las variables de la imagen del contenedor para que apunten a una imagen diferente con código no autorizado.

Apache Airflow, por su parte, solucionó muchos problemas de seguridad con la versión 2.0.0 que se lanzó en diciembre de 2020, por lo que es fundamental que los usuarios del software actualicen a la última versión y adopten prácticas de codificación seguras para evitar que las contraseñas estén expuestas.