Investigadores en ciberseguridad han identificado tres vulnerabilidades de seguridad en la integración de Apache Airflow en Azure Data Factory de Microsoft. Si estas vulnerabilidades se aprovechan con éxito, un atacante podría realizar acciones encubiertas como extraer datos confidenciales o desplegar malware.

> *«Explotar estas fallas permitiría a los atacantes mantener acceso persistente como administradores ocultos en todo el clúster de Azure Kubernetes Service (AKS) asociado a Airflow»,* explicó Unit 42 de Palo Alto Networks en un informe publicado recientemente.

Aunque Microsoft clasificó estas vulnerabilidades como de baja gravedad, las principales fallas identificadas son las siguientes:

1. Configuración incorrecta de los permisos RBAC (control de acceso basado en roles) en el clúster de Airflow.
2. Manejo defectuoso de secretos en el servicio interno Geneva de Azure.
3. Autenticación débil en el servicio Geneva.

Además de permitir el acceso no autorizado, un atacante podría explotar las debilidades en Geneva para alterar registros de actividad o generar registros falsos, evitando ser detectado al crear nuevos pods o cuentas.

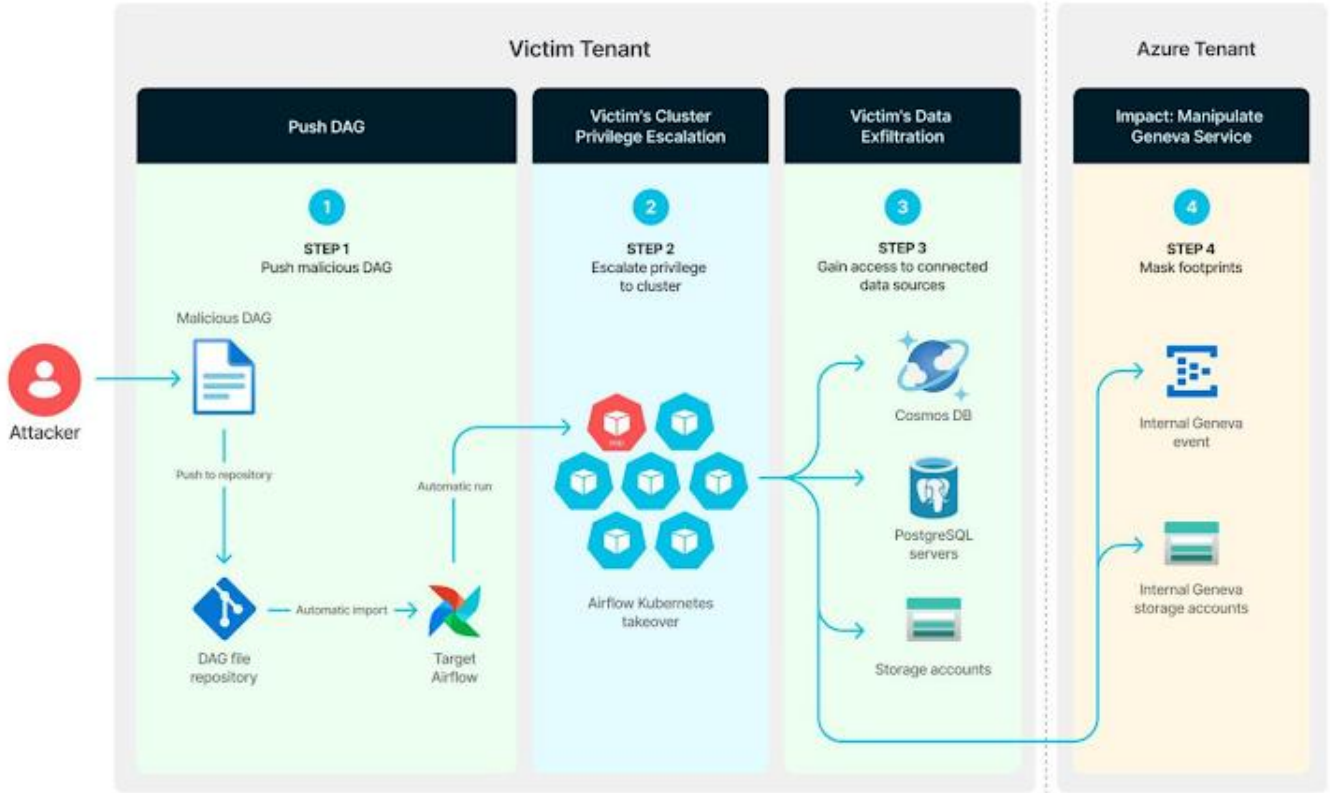
El método inicial de acceso consiste en diseñar un archivo DAG (grafo acíclico dirigido) y subirlo a un repositorio privado de GitHub conectado al clúster de Airflow, o modificar un archivo DAG ya existente. El objetivo final es ejecutar un shell inverso hacia un servidor externo tras la importación del archivo.

Para llevar a cabo este ataque, el actor malicioso primero necesitaría permisos de escritura en la cuenta de almacenamiento que contiene los archivos DAG, ya sea utilizando credenciales comprometidas de una entidad de servicio o un token de acceso compartido (SAS). Alternativamente, podrían comprometer un repositorio de Git utilizando credenciales

filtradas.

Aunque el shell obtenido de esta manera opera bajo el usuario de Airflow en un pod de Kubernetes con permisos limitados, un análisis más detallado reveló la existencia de una cuenta de servicio con permisos de administrador de clúster vinculada al pod de ejecución de Airflow.

Esta configuración incorrecta, combinada con la exposición del pod a internet, permitiría al atacante descargar la herramienta de línea de comandos kubectl y, finalmente, obtener control total sobre el clúster al *«desplegar un pod con privilegios elevados y acceder al nodo subyacente».*



El atacante podría utilizar el acceso root a la máquina virtual (VM) anfitriona para profundizar en el entorno de la nube, obteniendo acceso no autorizado a recursos internos gestionados por Azure, como Geneva, algunos de los cuales permiten realizar escrituras en cuentas de almacenamiento y concentradores de eventos.

> *«Esto implica que un atacante avanzado podría alterar un entorno de Airflow vulnerable. Por ejemplo, un atacante podría crear nuevos pods y cuentas de servicio adicionales. También sería capaz de modificar los nodos del clúster y enviar registros falsificados a Geneva sin activar alertas»,* explicaron los investigadores de seguridad Ofir Balassiano y David Orlovsky.
>
> *«Este incidente destaca la necesidad de gestionar con cuidado los permisos de servicio para evitar accesos no autorizados. También pone de manifiesto la importancia de supervisar las operaciones de servicios externos críticos para prevenir este tipo de intrusiones».*

Este hallazgo se produce mientras los laboratorios de seguridad de Datadog han descrito un caso de escalada de privilegios en Azure Key Vault que permitiría a los usuarios con el rol de «Key Vault Contributor» acceder o modificar datos del Key Vault, como claves API, contraseñas, certificados de autenticación y tokens SAS de Azure Storage.

El problema radica en que, aunque los usuarios con el rol «Key Vault Contributor» no tenían acceso directo a los datos del Key Vault configurado con políticas de acceso, se descubrió que dicho rol tenía permisos para añadirse a las políticas de acceso del Key Vault y, de este modo, acceder a los datos, eludiendo las restricciones existentes.

> *«Una actualización en las políticas podría incluir permisos para listar, visualizar, actualizar y administrar los datos dentro del Key Vault. Esto generaba un escenario donde un usuario con el rol de 'Key Vault Contributor' podía acceder a todos los*

> *datos del Key Vault, incluso sin tener permisos de [control de acceso basado en roles] para gestionar permisos o visualizar datos»*, señaló la investigadora de seguridad Katie Knowles.

Microsoft, por su parte, actualizó su documentación para señalar este riesgo relacionado con las políticas de acceso, afirmando: *«Para evitar accesos no autorizados y la administración de sus Key Vaults, claves, secretos y certificados, es crucial limitar el acceso del rol Contributor a los Key Vaults bajo el modelo de políticas de permisos de acceso».*

Además, recientemente se identificó un problema relacionado con los registros de Amazon Bedrock CloudTrail, que dificultaba distinguir entre consultas maliciosas y legítimas realizadas a modelos de lenguaje (LLMs), lo que permitía a actores malintencionados realizar análisis sin generar alertas.

> *«En particular, las llamadas fallidas a la API de Bedrock se registraban de forma idéntica a las exitosas, sin proporcionar códigos de error específicos»*, explicó Alessandro Brucato, investigador de Sysdig.
>
> *«La falta de información detallada sobre los errores en las respuestas de la API puede complicar la detección de amenazas, al generar falsos positivos en los registros de CloudTrail. Sin este nivel de detalle, las herramientas de seguridad podrían confundir actividades normales con sospechosas, provocando alertas innecesarias y posiblemente pasando por alto amenazas reales».*