Expertos en ciberseguridad han descubierto una vulnerabilidad de escalada de privilegios en Google Cloud que podría permitir que actores maliciosos manipulen las imágenes de aplicaciones e infecten a los usuarios, dando lugar a ataques en la cadena de suministro.

La vulnerabilidad, llamada Bad.Build, se encuentra en el servicio Google Cloud Build, según la empresa de seguridad en la nube Orca, que fue quien descubrió y reportó el problema.

> *«Al explotar esta falla y permitir una suplantación del servicio predeterminado de Cloud Build, los atacantes pueden manipular las imágenes en el Google Artifact Registry e introducir código malicioso»,* indicó la compañía en un comunicado.

> *«Cualquier aplicación creada a partir de las imágenes manipuladas se verá afectada y, si las aplicaciones defectuosas están destinadas a ser desplegadas en los entornos de los clientes, el riesgo se extiende desde el entorno de la organización proveedora hasta los entornos de los clientes, representando un riesgo importante para la cadena de suministro.»*

Después de una divulgación responsable, Google emitió una solución parcial que no elimina el vector de escalada de privilegios, describiéndolo como un problema de baja gravedad. No se requiere ninguna acción adicional por parte de los clientes.

El problema de diseño se origina en el hecho de que Cloud Build crea automáticamente una cuenta de servicio predeterminada para ejecutar compilaciones en nombre de los usuarios. Específicamente, esta cuenta de servicio tiene permisos excesivos («logging.privateLogEntries.list»), lo que permite el acceso a los registros de auditoría que contienen la lista completa de todos los permisos en el proyecto.

> *«Lo que hace que esta información sea tan valiosa es que facilita en gran medida el*

> *movimiento lateral y la escalada de privilegios en el entorno. Conocer qué cuenta de GCP puede llevar a cabo qué acción es equivalente a resolver una gran parte del rompecabezas sobre cómo lanzar un ataque»,* explicó el investigador de Orca, Roi Nisimi.

Al hacerlo, un actor malicioso podría explotar el permiso *«cloudbuild.builds.create»* ya obtenido de otras maneras para suplantar la cuenta de servicio de Google Cloud Build y obtener privilegios más elevados, extraer una imagen que se esté utilizando en Google Kubernetes Engine (GKE) y modificarla para incluir software malicioso.

> *«Nisimi explicó que una vez que se implementa la imagen maliciosa, el atacante puede aprovecharla y ejecutar código en el contenedor Docker con privilegios de root».*

Google implementó un parche que revoca el permiso *«logging.privateLogEntries.list»* de la cuenta de servicio de Cloud Build, evitando así el acceso para enumerar registros privados de forma predeterminada.

No es la primera vez que se reportan fallos de escalada de privilegios que afectan a la Plataforma de Google Cloud. En 2020, se detallaron diversas técnicas que podrían ser aprovechadas para comprometer entornos en la nube por parte de Gitlab, Rhino Security Labs y Praetorian.

Se recomienda a los clientes vigilar el comportamiento de la cuenta de servicio predeterminada de Google Cloud Build para detectar cualquier comportamiento malicioso posible, así como aplicar el principio de menor privilegio (PoLP) para reducir los posibles riesgos.