Google Cloud ha solucionado un defecto de seguridad de nivel medio en su infraestructura que podría ser explotado por un intruso que ya tuviera acceso a un clúster de Kubernetes para amplificar sus derechos de acceso.

> *«Si un atacante ha tomado el control del contenedor de registro Fluent Bit, podría aprovechar ese acceso junto con los permisos avanzados que necesita Anthos Service Mesh (en aquellos clústeres donde está activado) para incrementar sus capacidades dentro del clúster»*, indicó la empresa en un comunicado publicado el 14 de diciembre de 2023.

La unidad 42 de Palo Alto Networks, quien identificó y informó sobre el fallo, señaló que los ciberdelincuentes podrían utilizar esta vulnerabilidad para ejecutar acciones como *«exfiltrar información, instalar componentes maliciosos y perturbar el funcionamiento del clúster».*

No se ha detectado actividad maliciosa relacionada con esta falla hasta la fecha. Las versiones afectadas se han solucionado en las siguientes ediciones de Google Kubernetes Engine (GKE) y Anthos Service Mesh (ASM):

- 1.25.16-gke.1020000
- 1.26.10-gke.1235000
- 1.27.7-gke.1293000
- 1.28.4-gke.1083000
- 1.17.8-asm.8
- 1.18.6-asm.2
- 1.19.5-asm.4

Para que un atacante pueda aprovechar con efectividad este problema, es esencial que ya haya tomado el control de un contenedor FluentBit mediante otras vulnerabilidades, como podría ser una falla de ejecución de código a distancia.

```
/fluent-bit/bin/busybox-x86_64 cat <<"EOFF" > my_pod.yaml
apiVersion: v1
kind: Pod
metadata:
  name: pody
  namespace: kube-system
spec:
  containers:
  - name: pody
    image: yuvalavra/util:latest
    command: ["/bin/bash", "-c"]
    args:
    - |
        <******-attacker-code-to-escalate-privilege-to-cluster-admin-*******>
    volumeMounts:
    - name: shared-data
      mountPath: /shared-data
  volumes:
  - name: shared-data
    emptyDir: {}
  serviceAccountName: clusterrole-aggregation-controller
  automountServiceAccountToken: true
EOFF
```

Figure 6. Pod YAML file.

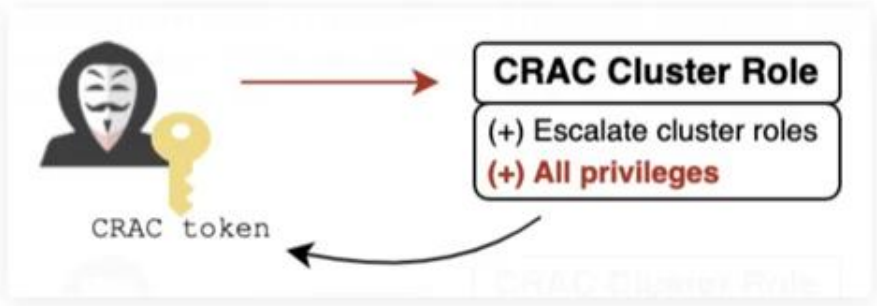

Figure 7. The CRAC token can add admin privileges to itself. Source: Container Escape To Shadow Admin: GKE Autopilot Vulnerabilities, Unit 42 article.

> *«Según detalló Google, GKE emplea Fluent Bit para analizar registros de tareas que se desempeñan en los clústeres. Además, en GKE, se había establecido Fluent Bit para registrar información de las tareas de Cloud Run. Al establecer este tipo de registro, Fluent Bit accedía a tokens de cuentas de servicio de Kubernetes de otros Pods presentes en el nodo.»*

Esto conllevaba que un atacante podría aprovechar dicho acceso para obtener mayores permisos en un clúster de Kubernetes con ASM activado, y posteriormente usar el token de ASM para amplificar sus capacidades al crear un pod con permisos de administrador del clúster.

> *«El servicio de agregación de roles de clúster (CRAC) se presenta como la opción principal, ya que tiene la habilidad de incorporar permisos adicionales a roles clúster existentes. Un atacante tendría la posibilidad de modificar el rol del clúster asociado a CRAC para obtener máximos privilegios»*, señaló el experto en seguridad Shaul Ben Hai.

Como medidas correctivas, Google ha restringido el acceso de Fluent Bit a los tokens de cuentas de servicio y ha modificado la estructura de ASM para reducir los permisos de control basado en roles (RBAC) exagerados.

> *«Cuando se inicia un clúster, los proveedores de nube generan de manera automática pods de sistema. Estos se integran en la infraestructura de Kubernetes, similar a los pods complementarios activados al implementar una característica específica»*, agregó Ben Hai.

> *«Esto se debe a que las entidades de nube o proveedores de aplicaciones son quienes generalmente los establecen y administran, limitando la intervención del usuario en sus ajustes o permisos. Esta situación representa un riesgo notable, dado que estos pods operan con privilegios elevados.»*