GKE (Google Kubernetes Engine) Kubernetes Attack(version 1.1)

**Cloud Service Label: IaaS, PaaS**

Description

Kubernetes is becoming extremely popular and due to containers being popular in the cloud this has led to many clients of providers such as GCP, AWS, and Azure utilizing Kubernetes to orchestrate containerized applications. Google Kubernetes Engine (GKE) is Google Cloud Platform’s Kubernetes management system. There are ways that an adversary might exploit GKE to perform privilege escalation.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Rhino Security Labs | Start with compromised GCP Credentials. Then list compute engine VM instances and log HTTP requests and responses. Then adversary would steal Kubelet bootstrap TLS credentials from the HTTP requests and responses log file that was listed. They would then submit certificate signing request to Kubernetes control plane, act as Kubernetes worker node, and steal Kubernetes secrets with worker node credentials; these steps can be repeated until the adversary is able to gain cluster-admin access. Once the cluster-admin access is gained they can list Kubernetes pods, execute into container, steal container service account, access the computer engine instance meta data server, steal GCP service account token, and access GCP cloud resources. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Two Factor Authentication | Use two factor authentication for user accounts. |
| Enable GKE Metadata Server | Consider enabling GKE Metadata Server which improves security and replaces Compute Engine VM instances Metadata Server. |
| Least Privilege | Use the concept of least privilege for management accounts. |

Detection

References

1. <https://cseweb.ucsd.edu/~savage/papers/CCS09.pdf>. Accessed July 2, 2020.