Google container security

Defense in depth for Kubernetes

Google Cloud gives you the ecosystem you need to develop and roll out software faster without compromising security; With Google Kubernetes, tenants can uniformly and seamlessly establish policy protection zones and let the system declaratively enforce them for you. You can also easily implement a defense-in-depth architecture with zero trust built into every layer.

Google container security

Containerization helps our development teams move fast, deploy software efficiently, and operate on an unprecedented scale. Google packaged over a decade's worth of experience, launching several billion containers per week into Google Cloud so that developers and businesses of any size can easily tap the latest in container innovation.

Out-of-the-box logging and monitoring

Kubernetes observability is available with no configuration through Google Kubernetes. Logs and telemetry automatically flow to Cloud Logging Cloud Monitoring, where clients can perform deep analyses, troubleshoot, set up alerts, create SLAs, and more.

Securing instances

With Google Cloud Platform, your projects take advantage of the same security model that Google uses to keep its customers safe on other Google properties. However, if your instance is configured incorrectly, it could be vulnerable to an attack. This is like how you need to keep the doors to your house locked, even though the police also patrol your neighborhood.

Clients should patch their docker container images in a matter of days. Since containers are immutable, they give you content addressability—they're stored in such a way that you are able to retrieve a container based on its contents.

From time to time, security issues in the container runtime, Kubernetes itself, or the node operating system might require you to upgrade your nodes more urgently. When you upgrade your node, the node's software is upgraded to their latest versions.

Known vulnerabilities within Google Containers

A known, challenging problem with the Kubernetes architecture is that there are so many Kubernetes distributions--and so many tools, philosophies and opinions within the Kubernetes ecosystem. The result is the platform strategy has become highly fractured.

Kubernetes Security is continuously being developed to keep pace with enhanced functionality, usability and flexibility while also balancing the security needs of a wide and diverse set of use-cases.

Recently, the GKE Security team discovered a high severity vulnerability that allowed workloads to have access to parts of the host filesystem outside the mounted volumes boundaries. Although the vulnerability was patched back in September, we thought it would be beneficial to write up a more in-depth analysis of the issue to share with the community.

A security researcher has disclosed the details of a vulnerability that can be exploited to take over virtual machines (VMs) on Google Cloud Platform.

Google's open door policy regarding security vulnerability discoveries

Google awards Uruguayan researcher $133,337 top prize in cloud security competition

A security researcher who discovered and exploited a remote code execution vulnerability in Google Cloud Deployment Manager has been crowned overall winner of Google's GCP VRP Prize 2020.

Using an internal version of the Google Cloud Platform (GCP) service, Uruguayan researcher Ezequiel Pereira issued requests to internal endpoints via Google's global software load balancer, as set out in the technical write-up that clinched the top prize.

This was the second year Google has run the GCP vulnerability reward program and offered six researchers a share of $313,337, or triple the $100,000 pool it created for the 2019 program. The prizes go to researchers who've submitted reports on exceptional security flaws in GCP. So this isn't a reward for a bug bounty, but an additional prize and recognition for submissions to Google vulnerability reward program.

The need for automated scanning of containers within Google

Google Container Analysis performs vulnerability scans on container images in Artifact Registry and Container Registry. It monitors the vulnerability information to keep it up to date. This process comprises two major tasks: scanning and continuous analysis.

Container Analysis scans new images when they're uploaded to Artifact Registry or Container Registry. This scan extracts information about the system packages in the container. The images are scanned only once, based on the image's digest. This means that adding or changing tags won't trigger new scans, only changing the contents of the image will.

Container Analysis only detects packages publicly monitored for security vulnerabilities.

Penetration Testing Google Containers and Kubernetes/Borg

Google cloud penetration testing is a recommended process for organizations that are considering cloud deployment for new or existing workloads. Penetration testing is a critical part of any security strategy, including on-premise and cloud deployments.

For penetration testing to be effective, it needs to be detailed and relevant. That means testing not just the application but also the all cloud and on-premise infrastructure.

Google private and public cloud penetration testing should include the following for any white box, gray box, or black box pen testing engagements:

- Identify security vulnerabilities
- Identify broken access controls
- What all things hackers can get from your google cloud?
- Real-life exploitation of security risks and vulnerabilities.
- Standard best practices to prevent security risks.

Does GCP allow penetration testing?

Google cloud began as a consumer product, not enterprise or service provider. The origins of their platform did not include several enterprise or government level security controls like FEDRAMP and ISO27001. These compliance frameworks became added years later. Even with billions of dollars invested along with having 500+ engineers worldwide, Google still lacks similar enterprise expertise that Microsoft Azure and Amazon web services have today. Google is making major head roads in the local and state government markets through having a secured cloud offering and compliance services. Tenants of Google still should incorporate 3rd party pen testing against their Google projects and VPC. Real-life exploitation of security risks and vulnerabilities will exist in some form within the Google cloud. Having an independent 3rd party

test team engage with your organization will ensure the highest level of objectivity and experience in validating the security within your Google instance.

Pen testing as part of Google open culture discovery for exploits and vulnerabilities

Frequent pen testing by a 3rd party team aligns with Google's open policy around discovery and reporting of vulnerability. The client should add pen testing more frequently as Google continues to make their cloud service offer more rich content and capabilities.

What makes CYBRI one of the Premier penetration testing companies?

Our outstanding penetration testing company services have attracted several clients that range from small startups to huge multinational companies. We are dedicated to improving cybersecurity across the board, which means that our services to your organization continue even after the pen test report has been delivered.

No matter the size of your organization, we will assess all of your cybersecurity needs from scratch to provide security measures tailored to your business needs. Our experts are always available to all of our clients in an advisory capacity should you wish to contact us.

Discuss your project with us!

Click here to go to our site, fill out the form and the engagement team will contact you shortly!
https://cybri.com/red-team/