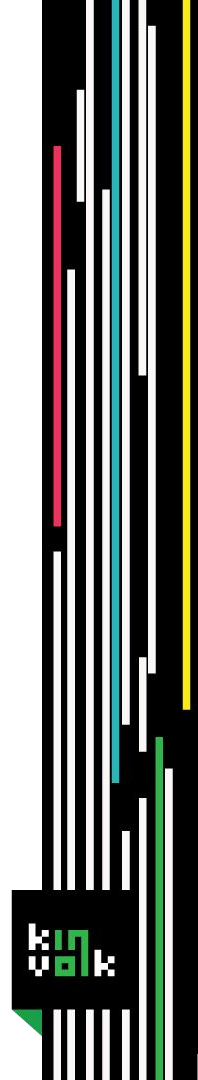
Applied Kubernetes Security

PITFALLS

Kubernetes today

- Many means available to make clusters more secure
- Continued efforts towards *secure-by-default*
- Fairly good security track record



CVE-2017-1002101 - subpath volume mount handling allows arbitrary file access in host filesystem #60813

New issue

Closed **liggitt** opened this issue on Mar 5 · 4 comments

liggitt commented on Mar 5 • edited ▾ Member ···

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

This vulnerability allows containers using subpath volume mounts with any volume type (including non-privileged pods, subject to file permissions) to access files/directories outside of the volume, including the host's filesystem.

Thanks to Maxim Ivanov for reporting this problem.

Vulnerable versions:

- Kubernetes 1.3.x-1.6.x
- Kubernetes 1.7.0-1.7.13
- Kubernetes 1.8.0-1.8.8
- Kubernetes 1.9.0-1.9.3

Assignees

liggitt

jsafrane

msau42

Labels

area/security

kind/bug

priority/critical-urgent

sig/storage

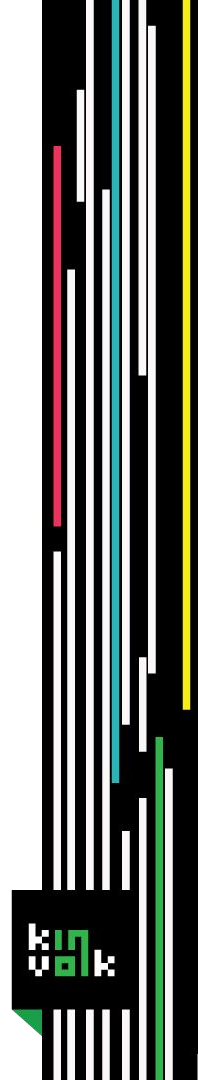
Projects

None yet

```
apiVersion: v1
kind: Pod
…
    volumeMounts:
    - mountPath: /test
      name: test
      subPath: malicious-symlink
  volumes:
  - name: test
    hostPath:
      path: /tmp/test
      type: Directory
```

“Complexity is insecurity”

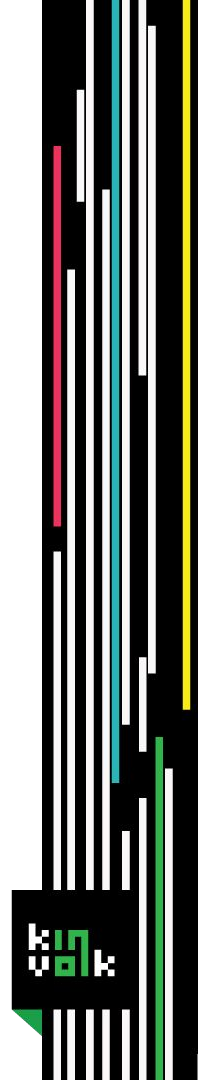
Complexity correlated with the presence of security vulnerabilities



Capture the flag

http://tiny.cc/k8sminictf

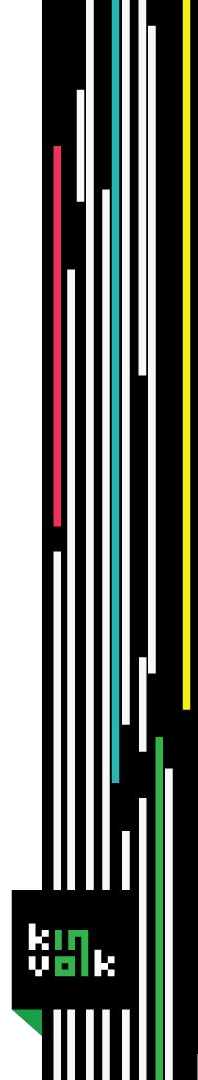
PS: No DoS and wrongdoing please :)



kube-apiserver: auth delegation

- Needed for e.g. API extensions

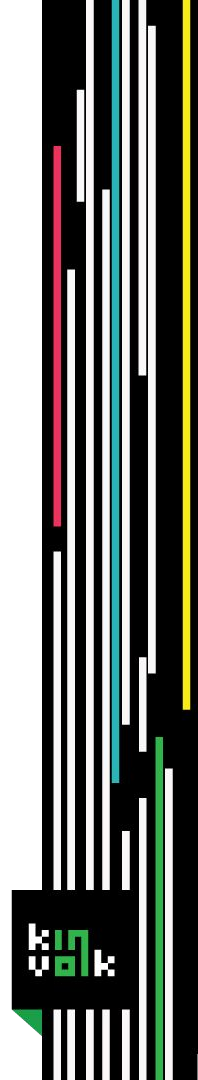
```
--requestheader-client-ca-file
--requestheader-group-headers
--requestheader-username-headers
--requestheader-allowed-names (~optional)
--requestheader-extra-headers-prefix (optional)
```



kube-apiserver: auth delegation

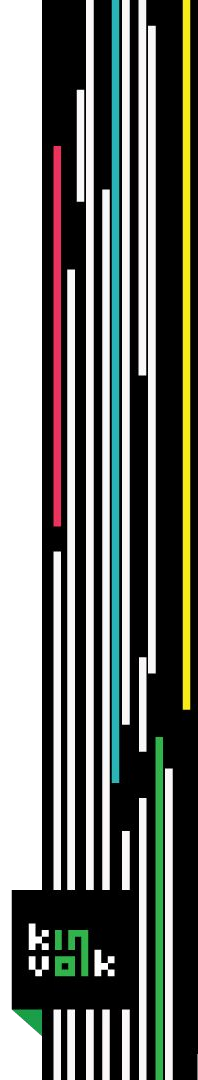
```
[Service]
ExecStart=/usr/local/bin/kube-apiserver \
  --authorization-mode=Node,RBAC \
  --client-ca-file=/etc/k8s/ca.pem \
  --bind-address=0.0.0.0 \
  […]
  --requestheader-client-ca-file=/etc/k8s/ca.pem \
  --requestheader-group-headers=X-Remote-Group \
  --requestheader-username-headers=X-Remote-User
```

CTF: Demo #1 http://tiny.cc/k8sminictf



PodSecurityPolicy (PSP)

- Added with v1.10
- Administrators decide what contexts pods can run in
- Would have been a way to mitigate CVE-2017-1002101 ... with the right policy

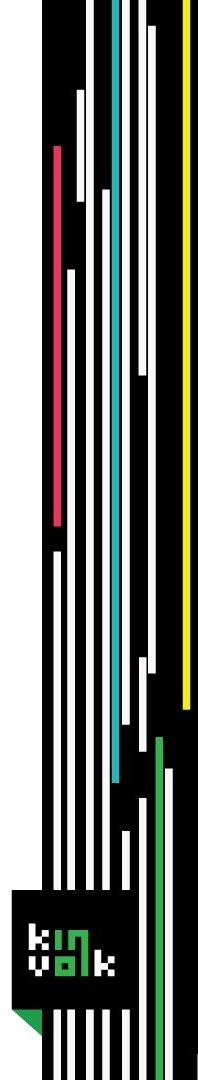


```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
…
  privileged: false
  volumes:
  - 'hostPath'
  allowedHostPaths:
    - pathPrefix: /tmp
  runAsUser:
    rule: 'MustRunAs'
    ranges:
    - min: 1
      max: 65535
```

CTF: Demo #2 http://tiny.cc/k8sminictf

Server-side request forgery (SSRF)

- “... is a type of exploit where an attacker abuses the functionality of a server causing it to access or manipulate information in the realm of that server ...”

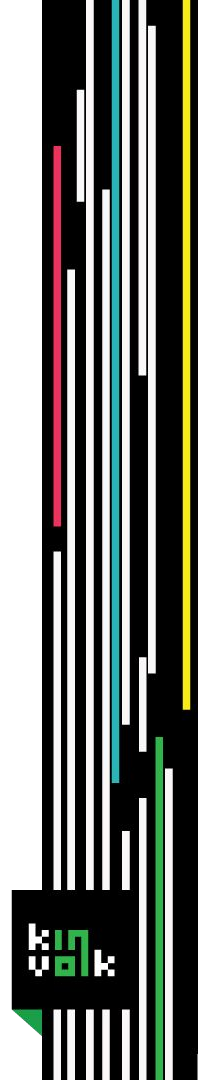


Server-side request forgery (SSRF)

```
<script>
window.location="http://metadata.google.internal/…;
</script>
```

https://hackerone.com/reports/341876

Kudos Shopify!



Thank you

hello@kinvolk.io

@schux00
@schu@chaos.social

michael@kinvolk.io

Resources

- https://github.com/kubernetes/kubernetes/issues/60813
- https://www.daemonology.net/blog/2009-09-04-complexity-is-insecurity.html
- https://www.schneier.com/blog/archives/2018/06/thomas_dullien_.html
- https://kubernetes.io/docs/concepts/policy/pod-security-policy/#volumes-and-file-systems
- https://en.wikipedia.org/wiki/Server-side_request_forgery
- https://hackerone.com/reports/341876