目录

修复runc漏洞CVE-2019-5736的公告

漏洞详情

runc是docker、containerd等容器的默认运行时环境。安全人员近日发现了runc的漏洞（CVE-2019-5736），恶意容器仅需要很少的用户操作就可以覆盖主机runc的二进制代码，并获取主机的root运行权限。

影响范围

对于金山云容器服务集群，Docker版本<18.09.2的所有kubernetes集群。

修复建议

若您使用的是金山云容器服务，您可以通过以下方法进行升级：

1、金山云容器服务已经修复了增量的版本，新创建的集群和新添加的节点已经包含了修复该漏洞的Docker版本，不受该漏洞影响。

2、对于存量的集群节点，升级runc文件（针对于Docker版本18.09.0）。可用root权限执行以下命令逐一升级集群节点上的runc二进制文件，此方法不影响该节点正在运行的业务。

以金山云容器集群v1.10.5版本为例：

i. 使用以下命令定位runc，金山云容器服务runc在：/usr/sbin/runc 路径下

```
which runc
```

ii. 备份原有的runc

```
mv /usr/sbin/runc /usr/sbin/runc.orig.$(date -Iseconds)
```

iii. 下载修复的runc

```
curl -o /usr/sbin/runc -sSL https://ks3-cn-beijing.ksyun.com/cve20195736/runc-v18.06.1-amd64
```

iv. 设置它的可执行权限

```
chmod +x /usr/sbin/runc
```

v. 测试runc可以正常工作

```
runc -v
# runc version 1.0.0-rc5+dev
# commit: 2bb99b3d44a1de2769866941e698f93f540b910c
# spec: 1.0.0
docker run -it --rm ubuntu echo OK
```