# sudo提权

CVE-2019-14287

1. **背景知识**

当在Linux操作系统上执行命令时，只有得到许可或者知道root密码，普通用户才可以使用sudo（super user do）命令以root身份执行命令。

因此对于sudo命令来说，通过向/etc/sudoers配置文件添加特殊的指令，就可以让某个用户以另一个用户的身份运行命令。

2019年10月14日， sudo 官方在发布了 CVE-2019-14287 的漏洞预警。它是由苹果信息安全部门的研究员 Joe Vennix 发现并分析的 。

Joe Vennix就在sudo上发现了一个[漏洞](https://www.sudo.ws/alerts/minus_1_uid.html)，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。

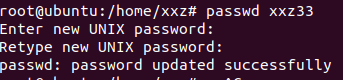
这是因为命令在将UID转换为对应用户时，会将-1或4294967295这两个异常数字视为0，而0是root用户的UID

**二、复现**

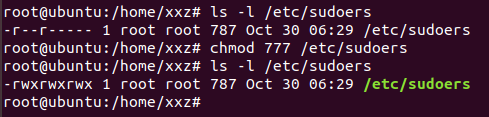
添加用户名xxz33



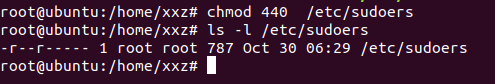
设置密码123456



一般情况/etc/sudoers为只读模式可以通过如图进行修改



然后用chmod 440 /etc/sudoers修改回来



也可以不修改直接通过visudo修改/etc/sudoers

修改前一般为：

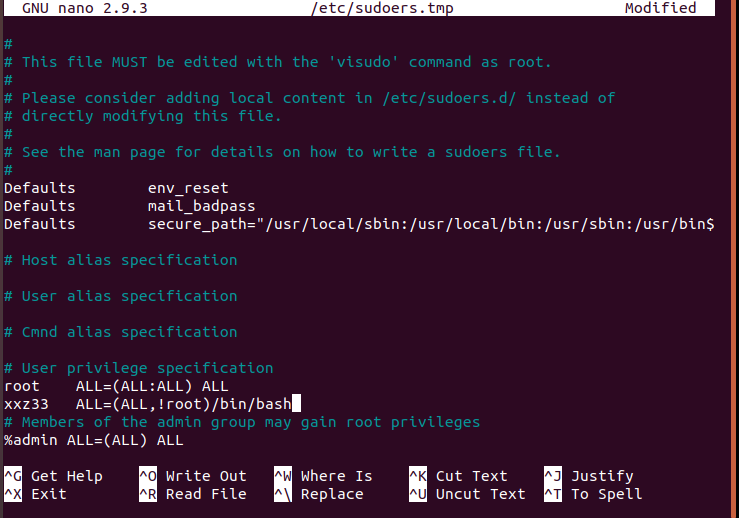
root ALL=(ALL:ALL) ALL

%wheel ALL=(ALL) ALL

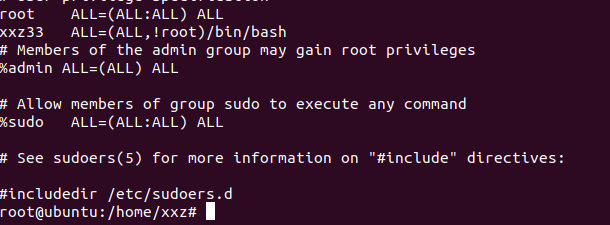
%sudo ALL=(ALL:ALL) ALL

找到root ALL=(ALL:ALL) ALL在他后进行修改格式为：

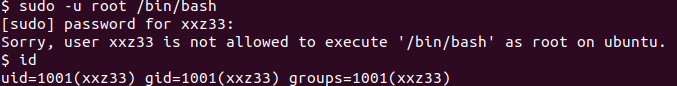
授权用户/组 主机=[(切换到哪些用户或组)] [是否需要输入密码验证] 命令1, [(字段3)] [字段4] 命令2, .



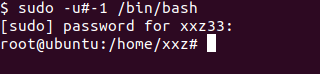
修改后为



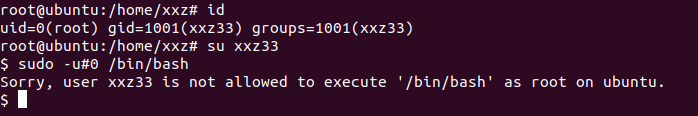
正常情况下为



利用漏洞可以做到



但如果是将-1改为0（root）的话依旧无法获得root权限



如果uid=1001（xxz33）则会变为



**三、分析与评价**

之所以会产生这个漏洞，是因为将用户 ID 转换为用户名的函数会将 -1（或无效等效的 4294967295）误认为是 0，而这正好是 root 用户 User ID 。此外，由于通过 -u 选项指定的 User ID 在密码数据库中不存在，因此不会运行任何 PAM 会话模块。

限制条件

1. Sudo版本低于1.8.28
2. 用户处于sudo权限列表之中
3. 知道用户的密码
4. 存在 ALL 关键词的复合限制逻辑

影响

1.8.28之前的Sudo版本。尽管该错误功能强大，但重要的是要记住，只有通过sudoers配置文件为用户提供了对命令的访问权限，它才能起作用。如果不是这样，并且大多数Linux发行版默认情况下都没有，那么此错误将无效。大多数Linux服务不受影响。360cert将其定为低危漏洞