Cve-2019-14287 **Sudo提权漏洞分析**

黄舒成 4042017009

1. 背景知识

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 。

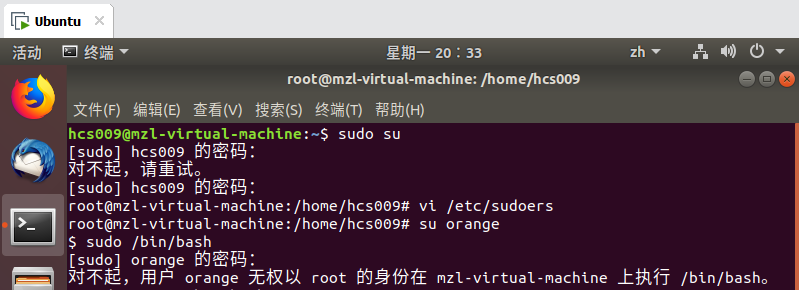
Linux是多用户多任务的操作系统, 共享该系统的用户往往不只一个。出于安全性考虑, 有必要通过useradd创建一些非root用户, 只让它们拥有不完全的权限; 如有必要再来提升权限执行。

sudo就是来解决这个需求的: 这些非root用户不需要知道root的密码，就可以提权到root，执行一些root才能执行的命令。

执行命sudo -u <用户名> <令>, 将允许当前用户，提权到<用户名>的身份，再执行后面的<命令>, 即使<命令>原本需要root权限。提权到<用户名>身份时，是以<用户名>的身份来执行命令的，因此创建的文件默认属于<用户名>用户。

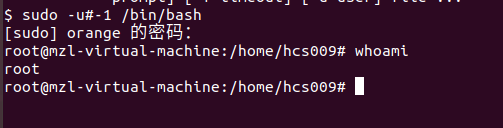
1. 漏洞复现

1.创建新用户orange后，添加sudo权限，orange用户不能使用root执行/bin/bash命令



Orange用户登陆，显示命令使用不成功

2.输入sudo -u#-1 /bin/bash 可执行成功



1. 漏洞原因

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：

Sudo版本低于1.8.28

知道用户的密码

用户处于sudo权限列表之中