# Linux sudo漏洞分析及复现

## 漏洞介绍

作为 Linux 中最常使用的重要实用程序之一，Sudo几乎安装在每一款 UNIX 和 Linux 发行版上，以便用户调用和实施核心命令。然而近期研究人员发现了一个提权漏洞，却直指Sudo的一个安全策略隐患——即便配置中明确不允许root用户访问，该漏洞仍可允许恶意用户或程序，在目标Linux系统上以root用户身份执行任意命令。Sudo（super user do）是用于类似Unix的计算机操作系统的程序，该程序允许用户使用其他用户的安全特权运行程序，默认情况下是超级用户。

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。

## 漏洞原理

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 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。简单来说，内核在处理时，会调用 prepare\_creds 函数创建一个新的凭证结构体，而传递给函数的 ruid、euid和suid 三个参数只有在不为 -1 的时候，才会将 ruid、euid 和 suid 赋值给新的凭证（见上面三个 if 逻辑），否则默认的 UID 就是 0。最后调用 commit\_creds 使凭证生效。这就是为什么传递 -1 时，会拥有 root 权限的原因。

补丁修复代码：

|  |  |
| --- | --- |
| 1 | /\* Disallow id -1, which means "no change". \*/if (!valid\_separator(p, ep, sep) || llval == -1 || llval == (id\_t)UINT\_MAX) { if (errstr != NULL) \*errstr = N\_("invalid value"); errno = EINVAL; goto done; } |

llval 变量为解析后的值，不允许 llval 为 -1 和 UINT\_MAX（4294967295）。

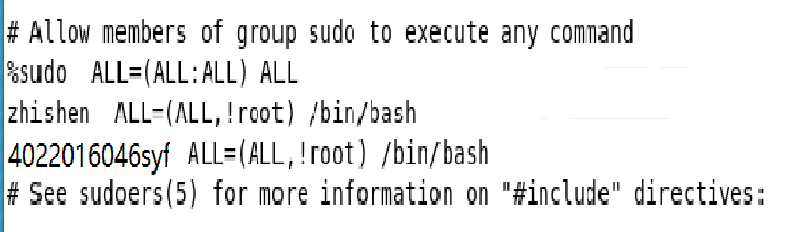
## 漏洞复现

1. 添加用户（为用户设置密码）

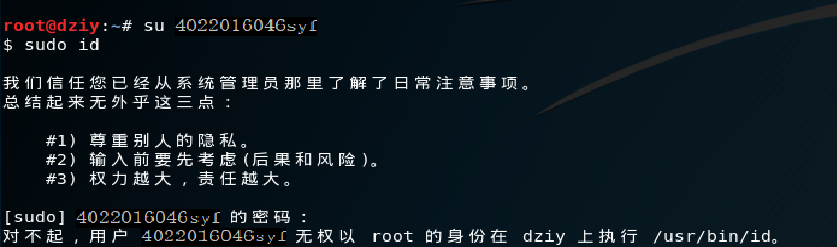
1root@MR6:~# useradd 4022016046syf

2root@MR6:~# passwd 4022016046syf  
3输入新的 UNIX 密码：  
4重新输入新的 UNIX 密码：  
5passwd：已成功更新密码

1. 在etc/sudoers文件中，添加相关修改



1. 进行提权的相关工作



4.提权

