# 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。

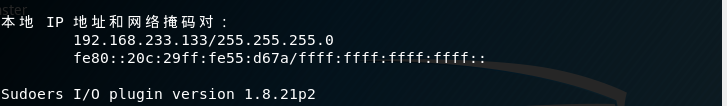
**二、漏洞原理**

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。

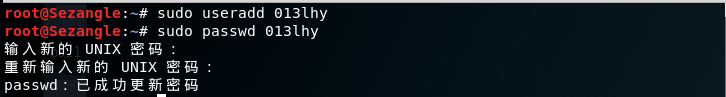
**三、漏洞复现**

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



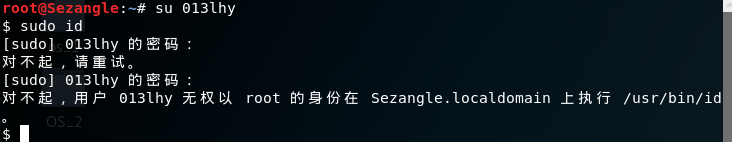
③配置sudoers文件

将创建的新用户加入sudoers中

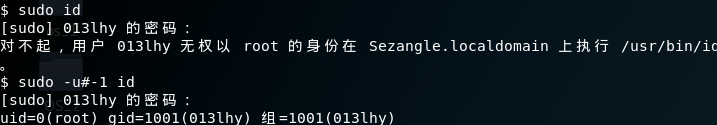


④使用用户并利用漏洞提权

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