# sudo提权

CVE-2019-14287

1. **背景**

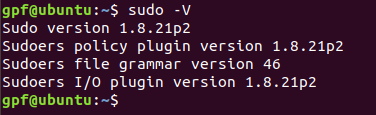
2019 年 10 月 14 日，CVE 官方发布了 CVE-2019-14287 的漏洞预警。它是由苹果信息安全部门的研究员 Joe Vennix 发现并分析的。 只要用户在使用sudo命令时指定UID为-1或4294967295，用户可提升至 root 权限（即使用 sudo 运行命令）。这是因为命令在将UID转换为对应用户时，会将-1或4294967295这两个异常数字视为0，而0是root用户的UID。

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。

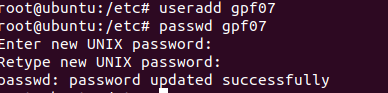
此漏洞复现起来较为简单，但环境较为落后，限制条件较为严苛。

1. **复现**

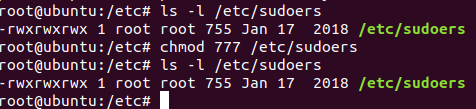
**检查sudo版本**

****

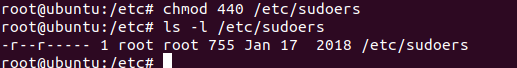
建立新用户gpf07



一般情况下当/etc/sudoers为只读模式可以通过下图进行修改

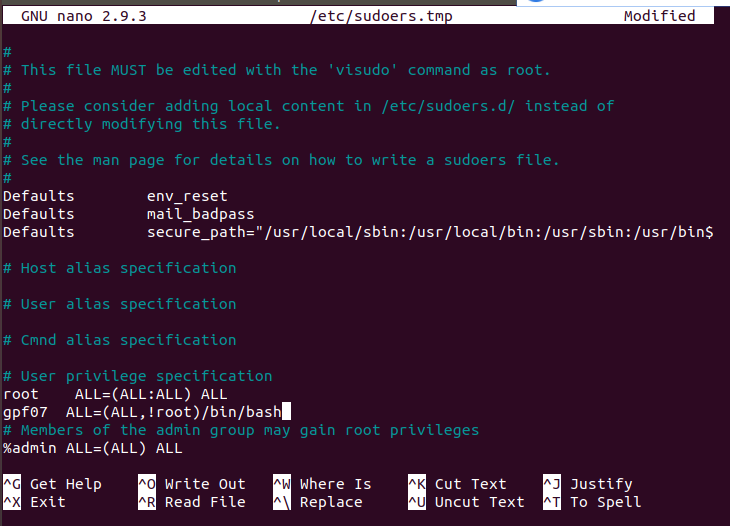


然后用chmod 440 /etc/sudoers修改回来

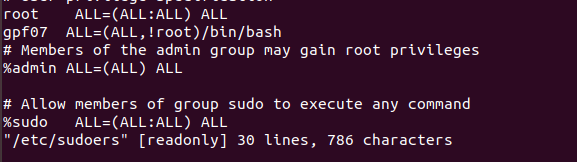


也可以不修改直接通过visudo修改/etc/sudoers

找到1573649486(1)在其后进行修改

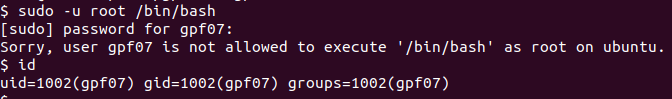


修改后为

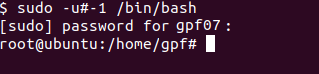


使用用户执行 sudo 命令：sudo id

正常情况下为



利用漏洞后



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。

**三、分析**

目前受影响的linux版本是小于1.8.28的sudo版本都会受到该漏洞的攻击,危害较大可导致服务器被攻击,被入侵,并提权,如果服务器里运行网站,APP,数据库的话,很有可能数据泄露,数据篡改等攻击问题的发生.

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