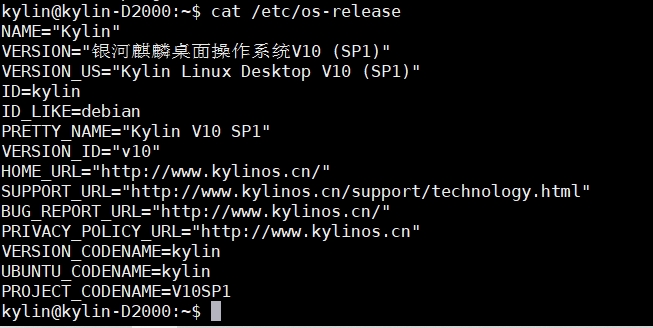
# Linux本地提权

## sudo相关漏洞

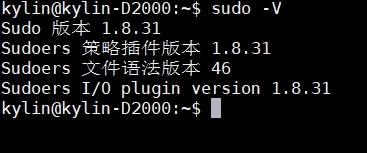
### CVE-2025-32462/32463 （√）

| 项目 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2025-32462 |
| 漏洞名称 | Linux sudo host 权限提升漏洞 |
| 影响版本 | Sudo 1.8.8 至 1.9.17 |
| 漏洞原理 | sudo 的 -h（--host）选项未严格限制必须与 -l（--list）选项配合使用，攻击者可伪造主机名参数，绕过 sudoers 文件中的主机访问控制规则，实现权限提升。 |
| 利用条件 | 攻击者需要在 sudoers 配置中有任意主机的授权（即存在可利用的主机相关权限配置）。 |
| 危害 | 攻击者可在非授权主机上以 root 权限执行任意命令，导致本地提权。 |
| 修复建议 | 升级 sudo 至安全版本，如 Sudo 1.9.17p1 及以上；同时检查 sudoers 配置，限制主机名参数的使用场景。 |

查看 Linux 系统的发行版信息



查看sudo版本信息



查看内核版本：

Linux 5.4.18-43-generic

1. 漏洞介绍

CVE-2025-32462 Linux sudo 本地权限提升漏洞在于 sudo 的 -h（--host）选项存在缺陷，该选项本应与 -l（--list）配合使用来查询远程主机权限，但实际未严格限制其仅用于查询功能，导致攻击者可能结合命令执行或文件编辑操作实现本地提权。

1. 影响范围

1.8.8 < Sudo版本 <= 1.9.17

本机sudo版本：1.8.31（符合）

1. 复现

使用的环境为Kylin V10 SP1，自带的sudo版本为1.8.31



执行sudo -i 提示需要密码和权限不够

编辑sudoers文件

sudo visudo #先sudo

visudo /etc/sudoers

在末尾添加：

|  |  |  |
| --- | --- | --- |
| cylin | ci.test.local | = NOPASSWD:ALL |
| 本机名 | 域名 | 权限分配 |

这一行的规则明确允许cylin用户在 ci.test.local上执行所有命令

sudo -i -h ci.test.local

CVE-2025-32463

| 项目 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2025-32463 |
| 漏洞名称 | Linux sudo chroot 权限提升漏洞 |
| 影响版本 | Sudo 1.9.14 至 1.9.17 |
| 漏洞原理 | sudo 的 -R（--chroot）选项在权限检查前提前解析用户指定的根目录，攻击者可构造恶意目录，内含伪造的 /etc/nsswitch.conf 文件，诱使 sudo 加载恶意动态库，进而绕过权限控制。 |
| 利用条件 | 攻击者可在可控目录中创建恶意 /etc/nsswitch.conf 文件，并通过 sudo -R <目录> 触发 chroot 环境加载该配置。 |
| 危害 | 攻击者可完全绕过权限限制，直接以 root 权限执行任意命令，实现本地提权。 |
| 修复建议 | 升级 sudo 至安全版本，如 Sudo 1.9.17p1 及以上；避免在不可信目录中使用 sudo -R 选项。 |

本机sudo版本为 1.8.31

### CVE-2025-6018/6019 （×）

| 项目 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2025-6018 |
| 漏洞名称 | Linux sudo 环境变量处理权限提升漏洞 |
| 影响版本 | Sudo 1.9.1 至 1.9.15p5、1.9.16 至 1.9.17p2（部分版本受影响，具体需参考官方公告） |
| 漏洞原理 | sudo 在处理特定环境变量（如与动态链接库加载相关的变量）时存在逻辑缺陷，未严格过滤或验证变量内容，导致攻击者可通过构造恶意环境变量，诱导 sudo 在执行命令时加载恶意动态库或篡改程序执行流程，进而绕过权限检查提权。 |
| 利用条件 | - 攻击者为本地低权限用户 - 系统 sudo 版本在受影响范围内 - 攻击者可控制部分环境变量的设置（通常低权限用户默认具备此能力） |
| 危害 | 允许本地低权限用户绕过 sudo 权限限制，以 root 身份执行任意命令，获取系统最高权限。 |
| 修复建议 | - 立即升级 sudo 至官方修复版本（如 1.9.18 及以上，具体以官方发布的安全版本为准） - 临时措施：在 /etc/sudoers 中通过 Defaults env\_reset 严格限制环境变量传递，减少漏洞利用可能性 |

CVE-2025-6019

| 项目 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2025-6019 |
| 漏洞名称 | Linux sudo 命令参数解析权限提升漏洞 |
| 影响版本 | Sudo 1.8.31 至 1.9.17p2（具体受影响版本需参考官方验证） |
| 漏洞原理 | sudo 在解析命令行参数（尤其是与用户切换、命令执行相关的参数组合）时存在语法解析错误，攻击者可通过构造特殊的参数序列（如嵌套的选项或畸形的命令路径），绕过 sudoers 文件中的命令白名单限制，执行未授权的高权限命令。 |
| 利用条件 | - 攻击者为本地低权限用户 - 系统 sudo 版本在受影响范围内 - /etc/sudoers 中存在基于特定命令的权限配置（即限制用户只能执行部分命令） |
| 危害 | 攻击者可突破 sudoers 中命令执行的限制，执行任意高权限命令，实现本地提权。 |
| 修复建议 | - 升级 sudo 至官方修复版本（如 1.9.18 及以上，具体以官方安全公告为准） - 临时措施：在 /etc/sudoers 中使用绝对路径严格限制可执行命令，避免模糊的命令配置（如禁止使用通配符） |

CVE-2025-6019 的触发依赖两个核心组件：

udisks2服务：版本存在权限校验缺陷，允许未授权的挂载操作。

libblockdev库：处理磁盘镜像时存在逻辑漏洞，可被利用构造恶意镜像。

要确保安装了受影响版本的 udisks 守护进程和 libblockdev 库。

udisks2 2.8.4-1kylin1

libblockdev 2.23.2kylin3

1、检查udisks2 服务及版本

udisks2是 Linux 系统中管理磁盘设备的服务，漏洞与此服务的权限控制相关。

Kylin 系统基于 Debian/Ubuntu 或 RHEL/CentOS 架构，分别使用dpkg或rpm查询：

# 若为Debian系（如Kylin V10 SP1）

dpkg -l | grep udisks2

# 若为RHEL系（如Kylin Server V10）

rpm -qa | grep udisks2

若输出结果包含udisks2，说明系统安装了该服务。

systemctl status udisks2

查询运行状态，需要是active时漏洞才可以触发

2、检查libblockdev 服务及版本

libblockdev是处理磁盘设备的底层库，漏洞与该库的镜像解析逻辑相关。

查看libblockdev安装情况及版本：

# Debian系

dpkg -l | grep libblockdev

dpkg -s libblockdev | grep Version

3、检查用户组权限（allow\_active相关）

漏洞利用需测试用户属于allow\_active组或具备类似权限（具体组名可能因系统配置略有差异），该组默认被授权进行磁盘管理操作。

输入groups进行群组检测

kylin adm cdrom sudo dip plugdev lpadmin sambashare

disk组：通常直接关联磁盘设备文件

storage组：部分发行版中用于统一管理存储设备权限

Plugdev （本机）

在多数 Linux 系统中，plugdev组的用户被允许挂载 / 管理外部存储设备（如 U 盘、移动硬盘），而udisks2正是负责这类设备管理的服务。因此，plugdev组权限可能已满足触发漏洞所需的基础设备操作权限。

4、验证系统是否允许用户挂载外部设备

CVE-2025-6019 的核心是低权限用户可绕过限制挂载恶意镜像，需确认系统是否允许普通用户执行挂载操作：

检查polkit配置（udisks2依赖polkit进行权限控制）：

# 查看udisks2的polkit权限配置

cat /usr/share/polkit-1/actions/org.freedesktop.UDisks2.policy | grep -A 10 "mount"

若配置中允许allow\_active组用户执行org.freedesktop.udisks2.filesystem-mount等动作（如result\_active=yes），则符合漏洞触发的权限条件。

提示结果如下 :

<defaults>

<allow\_any>auth\_admin</allow\_any> <allow\_inactive>auth\_admin</allow\_inactive>

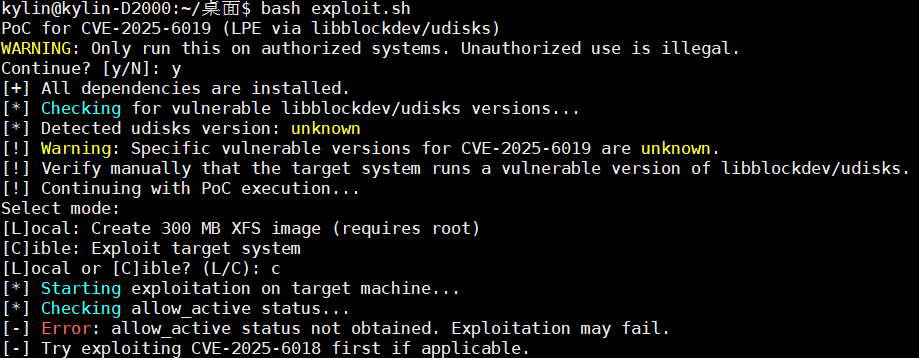
<allow\_active>yes</allow\_active>

</defaults>

<allow\_active>yes</allow\_active>

对于已认证且会话激活的用户（即当前登录并活跃使用系统的用户），允许直接执行该动作，无需额外认证。

意味着当前活跃用户（如你所在的kylin用户）无需管理员密码即可执行挂载操作，这正好满足漏洞利用所需的 “低权限用户可操作存储设备” 的基础条件。



## 内核相关漏洞

### CVE-2023-32629 （×）

|  |  |
| --- | --- |
| 项目 | 详情 |
| 漏洞编号 | CVE-2023-32629 |
| 漏洞名称 | Linux 内核 OverlayFS 权限检查绕过漏洞 |
| 影响版本 | 6.2.0（Ubuntu 23.04 (Lunar Lobster) ）  5.19.0（Ubuntu 23.04 (Lunar Lobster) ）  5.4.0（Ubuntu 23.04 (Lunar Lobster) ） |
| 漏洞原理 | Linux 内核 OverlayFS 实现在检查trusted.overlayfs.\*扩展属性时存在权限检查绕过，允许本地用户通过构造特定文件系统操作提升权限 |
| 利用条件 | 攻击者为本地用户 系统使用受影响版本的内核及 OverlayFS 组件 |
| 危害 | 本地用户可利用该漏洞提升权限，获取更高权限操作，对系统安全造成威胁 |

uname -rs查询内核信息

Linux 5.4.18-43-generic

不符合条件

在进行OverlayFS 挂载层的写入时权限受限。



### CVE-2025-38236（×）

[POC](https://cn-sec.com/archives/4263570.html) EXP（无）

攻击者可利用该漏洞从Linux系统的Chrome渲染器沙箱内实现权限提升

| 信息项 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2025-38236 |
| 漏洞名称 | Linux Kernel AF\_UNIX UAF 漏洞 |
| 披露时间 | 2025-07-08 |
| 影响范围 | 由 Linux Kernel 5.15 版本引入该问题。具体影响 Linux Kernel 6.1.142 及更早版本、Linux Kernel 6.6.95 及更早版本、Linux Kernel 6.12.35 及更早版本、Linux Kernel 6.15.4 及更早版本、Linux Kernel 6.9及以上版本 |
| 漏洞描述 | 该漏洞存在于 AF\_UNIX 套接字处理 MSG\_OOB（带外数据）时的逻辑缺陷中。当应用程序以特定顺序读取 OOB 数据时，会导致内核出现 use - after - free 内存错误。具体过程为：应用使用 MSG\_OOB 标志读取数据时，数据不会从 receive 队列中删除；当发送新的 OOB 数据后，若应用未使用 MSG\_OOB 标志读取数据，会因特定逻辑导致队列中数据处理异常，使得 oob\_skb 成为悬空指针，再次使用 MSG\_OOB 标志读取数据时，就会指向已释放的内存，从而引发 UAF。 |
| 漏洞利用方式 | 攻击者可通过泄露内核地址信息，利用悬空指针实现受控内存读写，进而完成权限提升，甚至可从 Chrome 渲染器沙箱内实现权限提升，建立读取原语将任意内核内存复制至用户空间，绕过用户拷贝加固限制。 |

当前设备linux内核版本为5.4.18-43-generic，不在漏洞范围内

### CVE-2024-1086（×）

[EXP](https://www.ddosi.org/cve-2024-1086/" \l ":~:text=CVE-2024-1086%20%E7%9A%84%E9%80%9A%E7%94%A8%E6%9C%AC%E5%9C%B0%E6%9D%83%E9%99%90%E6%8F%90%E5%8D%87%E6%BC%8F%E6%B4%9E%E6%A6%82%E5%BF%B5%E9%AA%8C%E8%AF%81%EF%BC%8C%E9%80%82%E7%94%A8%E4%BA%8E%20v5.14%20%E5%92%8C%20v)

[blog](https://pwning.tech/nftables/)

| 信息类别 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2024-1086 |
| 漏洞名称 | Linux kernel 权限提升漏洞 |
| 漏洞类型 | 释放后使用（Use - After - Free）漏洞 |
| 影响范围 | Linux 内核 3.15 至 6.8-rc1 版本，具体为 3.15≤Linux kernel＜6.1.76、5.2≤Linux kernel＜6.6.15、6.7≤Linux kernel＜6.7.3 以及 Linux kernel=6.8:rc1；不适用于内核配置CONFIG\_INIT\_ON\_ALLOC\_DEFAULT\_ON=y且 Linux 内核版本 > 6.4 的系统 |
| 漏洞位置 | Linux 内核的 netfilter 子系统的 nf\_tables 组件 |
| 漏洞原理 | nft\_verdict\_init () 函数允许将正值作为 hook verdict 中的 drop 错误，当使用类似于 NF\_ACCEPT 的 drop 错误来发出 NF\_DROP 命令时，nf\_hook\_slow () 函数可能会导致双重释放漏洞，从而可被本地攻击者利用进行提权 |
| 危害后果 | 本地攻击者可利用该漏洞将权限提升为 root，获取目标服务器的最高管理权限 |
| 修复建议 | 升级到 Linux 内核 v5.15.149、v6.1.76、v6.6.15 或更高版本；也可升级到经过修补的特定版本 |

该漏洞不适用于带有 kconfig 的 >v6.4 内核

CONFIG\_INIT\_ON\_ALLOC\_DEFAULT\_ON=y

判断：查看 /proc/config.gz或 /boot/config-$(uname -r)文件：

zcat /proc/config.gz | grep CONFIG\_INIT\_ON\_ALLOC\_DEFAULT\_ON

该漏洞利用需要用户命名空间 (kconfig CONFIG\_USER\_NS=y)，这些用户命名空间没有特权(sh command sysctl kernel.unprivileged\_userns\_clone= 1)，并且 nf\_tables 已启用 (kconfig CONFIG\_NF\_TABLES=y)。

检查 CONFIG\_USER\_NS和 CONFIG\_NF\_TABLES​​

zcat /proc/config.gz | grep -E "CONFIG\_USER\_NS|CONFIG\_NF\_TABLES"

检查用户命名空间权限​

sysctl kernel.unprivileged\_userns\_clone

确认 nf\_tables模块状态​

lsmod | grep nf\_tables



### CVE-2025-21756（×）

Linux内核微小漏洞引发完整Root提权攻击

| 信息类别 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2025-21756 |
| 漏洞类型 | 释放后重用（Use - After - Free，UAF）漏洞 |
| 影响范围 | 具有 vsock（虚拟套接字）实现的 Linux 内核，特别是 6.6.79、6.12.16、6.13.4 和 6.14 - rc1 之前的版本 |
| 漏洞成因 | 传输重分配期间对套接字绑定状态处理不当，vsock 代码错误地减少了已解绑套接字的引用计数器，导致 vsock 对象过早释放 |
| 漏洞利用前提条件 | 本地访问，能够创建和操作 vsock 套接字；攻击者必须拥有本地权限，攻击复杂度低，无需用户交互 |
| 漏洞利用方法 | 通过触发 UAF 漏洞，利用管道支持页面覆盖关键内核结构；利用 vsock\_diag\_dump () 作为侧信道泄露 init\_net 的内存地址，绕过内核地址空间布局随机化（KASLR）；构建 ROP 链调用 commit\_creds (init\_cred) 来提升权限，通过调用套接字的 release () 函数触发 sk->sk\_error\_report 的函数指针覆盖来重定向执行 |
| 影响后果 | 攻击者可获得 root 权限，可能导致系统被入侵、数据被盗或服务中断 |
| 修复建议 | 将系统更新至最新内核版本，对于无法立即修补的系统，建议限制本地用户访问并监控与 vsock 子系统相关的可疑活动 |

VSOCK（Virtual Socket） 是一种专为虚拟机（VM）与宿主机之间高效通信设计的套接字协议，由 VMware 最初提出并集成到 Linux 内核中。

unaffected from 0 before 5.5  本机linux版本不受影响

### CVE-2024-26809（×）

poc：<https://github.com/otter-sec/OtterRoot/blob/master/universal/exploit.c>

[OtterRoot Netfilter 通用型 Linux 本地提权](https://cn-sec.com/archives/3537458.html)

| 信息项 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2024-26809 |
| 漏洞名称 | Linux 内核 nftables 子系统双重释放漏洞 |
| 影响范围 | Linux 内核版本 6.1-rc1 及以上以及 5.15.54 及以上的系统 |
| 漏洞类型 | 双重释放（double-free） |
| 漏洞描述 | 该漏洞源于 Linux 内核 nftables 数据包过滤功能中 pipapo 集合销毁过程的逻辑缺陷。在特定条件下，某个元素可能同时存在于 match 和 clone 中，当 dirty 标志被设置时，nft\_pipapo\_destroy () 函数会对重叠的内存区域错误地调用两次 nft\_set\_pipapo\_match\_destroy ()，导致对同一内存区域执行两次释放操作，从而引发内存损坏。 |
| 利用方式 | 攻击者通过内核对象缓存系统 kmalloc-256 进行堆布局和操控，精心设计内存分配与释放操作，实现重叠 nftables 对象、泄露内核地址、劫持函数指针（如 expr->ops->dump），并执行 ROP（返回导向编程）指令链获取 root 权限。 |

### CVE-2022-0847（×）

| 信息项 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2022-0847 |
| 漏洞名称 | Dirty Pipe（脏管道）漏洞 |
| 漏洞类型 | 变量未初始化 |
| 影响范围 | 5.8<=Linux Kernel 版本 < 5.16.12/5.15.25/5.10.102 |
| 漏洞描述 | Linux 内核的 copy\_page\_to\_iter\_pipe 和 push\_pipe 函数中，新管道缓冲区结构的 “flags” 成员缺乏正确初始化，可包含陈旧值。非特权本地用户可利用此缺陷向只读文件支持的页面缓存写入数据，从而提升其在系统上的权限。 |
| 漏洞利用方式 | 攻击者通过构造特定的管道操作，利用未初始化的 flags 成员，将文件缓存页当作普通管道缓存页进行续写和篡改，由于内核不会将这个缓存页判定为 “脏页”，所以在原缓存页有效期内，所有访问该文件的场景都将使用被篡改的文件缓存页，实现对任意可读文件的写操作，进而完成本地提权。 |
| 修复建议 | 更新 Linux 内核至 5.16.12、5.15.25 或 5.10.102 及以上版本。 |

## 其他服务相关漏洞

### CVE-2025-27591（×）

| 信息项 | 详情 |
| --- | --- |
| 漏洞编号 | CVE-2025-27591 |
| 漏洞名称 | Linux Below 服务权限提升漏洞 |
| 披露时间 | 2025 年 3 月 31 日（第三方安全社区首次披露） |
| 影响范围 | Below 服务版本 < v0.9.0 |
| 漏洞类型 | 权限提升（Privilege Escalation） |
| 漏洞描述 | 该漏洞源于/var/log/below目录被设置为全局可写（权限 777）。攻击者可通过创建符号链接将日志文件指向敏感文件（如/etc/shadow），当 Below 服务以 root 权限写入日志时，会间接修改目标文件，最终实现权限提升至 root。 |
| 利用条件 | 1. 目标系统运行 Below 服务且版本低于 v0.9.0 2. 攻击者拥有本地非特权用户权限 |
| 利用步骤 | 1. 创建符号链接：ln -s /etc/shadow /var/log/below/attack.log 2. 触发服务写入日志，覆盖或修改敏感文件内容 |
| 修复建议 | 1. 升级 Below 服务至 v0.9.0 或更高版本 2. 手动设置目录权限：chmod 700 /var/log/below |

Below是由Facebook开源的一款Linux系统资源监控工具

