Linux 内核权限提升漏洞（CVE-2024-1086）通告

■ **通告编号**	**NS-2023-0010-1**	■ 发布日期	**2024-03-29**
■ **漏洞危害**	**攻击者利用此漏洞，可实现系统权限提升。**		
■ **TAG**	Linux、kernel、CVE-2024-1086、PoC 已公开		

一. 漏洞概述

近日，绿盟科技 CERT 监测网上有研究员公开披露了一个 Linux 内核权限提升漏洞（CVE-2024-1086）的细节信息与验证工具，由于 Linux 内核的 netfilter：nf_tables 组件存在释放后重利用漏洞， nft_verdict_init() 函数允许在钩子判定中使用正值作为丢弃错误，当 NF_DROP 发出类似于 NF_ACCEPT 的丢弃错误时，nf_hook_slow() 函数会导致双重释放漏洞，本地攻击者利用此漏洞可将普通用户权限提升至 root 权限。目前漏洞 PoC 公开，请相关用户尽快采取措施进行防护。

Netfilter 是 Linux 内核提供的一个框架，它允许以自定义处理程序的形式实现各种与网络相关的操作。Netfilter 为数据包过滤、网络地址转换和端口转换提供了各种功能和操作，它们提供了通过网络引导数据包和禁止数据包到达网络中的敏感位置所需的功能。

参考链接：

https://bugzilla.redhat.com/show_bug.cgi?id=2262126

二. 影响范围

受影响版本

- 3.15 <= Linux kernel < 6.1.76
- 6.2 <= Linux kernel < 6.6.15
- 6.7 <= Linux kernel < 6.7.3
- Linux kernel = 6.8-rc1

注：已知 Redhat、Ubuntu、Debia 等 Linux 发行版受影响

不受影响版本

- Linux kernel = 4.19.307
- Linux kernel = 5.4.269
- Linux kernel = 5.10.210
- Linux kernel = 5.15.149
- Linux kernel >= 6.1.76

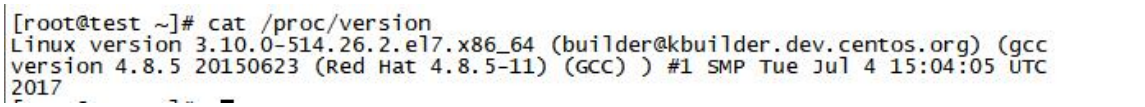
- Linux kernel >= 6.6.15
- Linux kernel >= 6.7.3
- Linux kernel >= 6.8-rc2

三. 漏洞检测

3.1 版本检测

Linux 系统用户可以通过查看版本来判断当前系统是否在受影响范围内，查看操作系统版本信息命令如下：

```
cat /proc/version
```



四. 漏洞防护

4.1 官方升级

目前官方已升级内核版本修复该漏洞，请受影响的用户尽快更新版本进行防护，官方下载链接：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f342de4e2f33e0e39165d8639387aa6c19dff660

Redhat：https://access.redhat.com/security/cve/CVE-2024-1086

Ubuntu：https://ubuntu.com/security/CVE-2024-1086

Debian：https://security-tracker.debian.org/tracker/CVE-2024-1086

Centos：https://lists.centos.org/pipermail/centos-announce/2024-March/099235.html

统信：https://src.uniontech.com/#/security_advisory_detail?utsa_id=UTSA-2024-000633

麒麟：https://kylinos.cn/support/loophole/patch/5561.html

4.2 其他防护措施

若相关用户暂时无法进行升级更新，可使用以下措施进行临时防护：

1、如果业务不需要，可以通过阻止加载受影响的 netfilter（nf_tables）内核模块来缓解。

```
RedHat/CentOS：
# echo 'blacklist nf_tables' >> /etc/modprobe.d/blacklist-nf_tables.conf
# dracut -f
# reboot

Debian/Ubuntu：
# sudo echo 'blacklist nf_tables' >> /etc/modprobe.d/blacklist-nf_tables.conf
# sudo update-initramfs -u
# reboot
```

有关如何将内核模块列入黑名单的说明，请参阅 https://access.redhat.com/solutions/41278。

2、如果无法禁用该模块，用户可在 Linux 非容器化部署中，对 user_namespace（用户命名空间）进行限制。

```
RedHat/CentOS：
# echo "user.max_user_namespaces=0" > /etc/sysctl.d/userns.conf
# sysctl -p /etc/sysctl.d/userns.conf

Debian/Ubuntu：
临时禁用：
# sudo sysctl -w kernel.unprivileged_userns_clone=0
永久禁用：
# echo kernel.unprivileged_userns_clone=0 | sudo tee /etc/sysctl.d/99-disable-unpriv-usern
s.conf
```

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。