Linux Kernel权限提升漏洞(CVE-2023-32233)通告

■ **通告编号**	**NS-2023-00**	■ 发布日期	**2023-05-17**
■ **漏洞危害**	**攻击者利用漏洞可实现权限提升**		
■ **TAG**	Linux、Kernel、Netfilter nf_tables、CVE-2023-32233、权限提升		

一. 漏洞概述

近日，绿盟科技 CERT 监测发现网上公开披露了 Linux Kernel 权限提升漏洞(CVE-2023-32233)的 PoC。由于 Linux 内核的子系统 Netfilter nf_tables 中存在 use-after-free 漏洞，在处理批处理请求时存在缺陷，经过身份验证的本地攻击者可利用该漏洞在内核内存中进行任意读写操作，最终可实现将权限提升至 ROOT。CVSS 评分为 7.8，请受影响的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。

CVE-2023-32233 漏洞状态：

漏洞细节	漏洞 PoC	漏洞 EXP	在野利用
已公开	已公开	已公开	暂未监测到

参考链接：

https://www.openwall.com/lists/oss-security/2023/05/15/5

二. 影响范围

受影响范围

- Linux Kernel <= 6.3.1

不受影响范围

- Linux kernel > 6.3.1

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
```

```
[root@test ~]# cat /proc/version
Linux version 3.10.0-514.26.2.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc
version 4.8.5 20150623 (Red Hat 4.8.5-11) (GCC) ) #1 SMP Tue Jul 4 15:04:05 UTC
2017
```

四. 漏洞防护

4.1 补丁更新

1. 目前官方已发布安全版本修复此漏洞，建议受影响的用户及时安装防护，下载链接：https://kernel.org/

2. 同时也可以下载 Linux 系统内核补丁的方式进行防护，相关链接：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=c1592a89942e9678f7d9c8030efa777c0d57edab

3. 目前主流 Linux 发行版已发布安全补丁或更新版本修复此漏洞，建议用户尽快安装补丁或参照官方措施进行防护：

Linux 发行版	官方通告
Ubuntu	https://ubuntu.com/security/CVE-2023-32233
Debain	https://security-tracker.debian.org/tracker/CVE-2023-32233
Redhat	https://access.redhat.com/security/cve/CVE-2023-32233

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。