# 安全通告

## 关于 Linux kernel 存在权限提升漏洞的预警通报

发布日期：2024-6-7

[2024]009 号

**漏洞描述**

2024 年 6 月 7 日公司监测到，Linux kernel 存在远程代码执行漏洞（CVE-2024-1086）。Netfilter 是 Linux 内核中的一个数据包处理模块，它可以提供数据包的过滤、转发、地址转换 NAT 功能。该漏洞主要是由于 Netfilter 模块的 nf_tables 子系统中存在释放后重用（Use-After-Free）问题，导致在本地经过身份验证的攻击者（包含具有低权限的用户）可以利用该缺陷提升到 root 权限。

**漏洞编号**

CVE-2024-1086

**漏洞危害**

攻击者可能利用这一漏洞在受影响的系统上从低权限账号提升至 root 权限。

**漏洞等级**

高危

**受影响版本**

5.2 ≤ Linux kernel < 6.6.15

6.7 ≤ Linux kernel < 6.7.3

linux kernel = 6.8-rc1

**修复方案**

官方已发布了漏洞修复方案，请及时关注更新：

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f342de4e2f33e0e39165d8639387aa6c19dff660

Ubuntu 修复方案：

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

Centos 修复方案：

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

RedHat 修复方案：

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

Debian 修复方案：

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

统信修复方案：

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

麒麟修复方案：

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

**参考链接**

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1086