网络安全预警通报

2026 年第 3 期（总第 61 期）

西安交通大学网络信息中心 2026 年 04 月 30 日

【预警类型】高危预警

【预警内容】

Linux 内核“Copy Fail”本地提权漏洞（CVE-2026-31431）高危利用风险通报

一、漏洞概述

近日，安全研究人员披露了 Linux 内核中存在近十年的高危本地提权漏洞，代号为“Copy Fail”，漏洞编号为 CVE-2026-31431。该漏洞存在于 Linux 内核的 crypto 子系统 authencesn 加密模板中，源于 2017 年引入的一个逻辑优化缺陷。攻击者仅需一个 732 字节的 Python 脚本，即可从普通用户权限直接提升至 root 权限，且无需竞态条件、无需内核特定偏移，利用方式极为稳定可靠。

该漏洞自 2017 年以来影响所有主流 Linux 发行版，包括 Ubuntu、Debian、RHEL、Fedora、SUSE 等。受影响的系统覆盖了几乎所有生产环境、开发测试环境以及容器化部署场景。同时，由于漏洞通过

页面缓存（page cache）写入实现篡改，可绕过磁盘文件完整性校验，并能跨越容器隔离边界，导致容器内低权限进程可直接攻破宿主机。

目前公开渠道已可获取完整的漏洞利用代码，攻击门槛极低，预计将很快出现大规模自动化扫描和利用行为。建议各单位立即开展排查和加固工作。

二、漏洞详情

1.技术原理

漏洞编号：CVE-2026-31431

漏洞名称：Copy Fail

漏洞类型：内核逻辑缺陷 → 本地提权

漏洞等级：高危

公开日期：2026 年 4 月 29 日

产生原因：

2017 年 Linux 内核进行了一项优化（commit 72548b093ee3），试图让 AEAD 加解密操作直接在原地完成以减少内存拷贝。然而在解密路径中，系统错误地将文件页缓存页面与加解密缓冲区混用，攻击者可通过 AF_ALG 密码算法接口和 splice()系统调用，向内核页缓存中写入 4 个可控字节。

2.利用条件

- 本地存在普通用户账号（无需特殊权限）
- Linux 内核版本为 2017 年至修复补丁之间的任意版本

- 内核 crypto API（AF_ALG）在默认配置中通常开启
- 系统存在 setuid 二进制文件（如/usr/bin/su、/usr/bin/sudo 等）

三、漏洞影响范围

1.受影响版本

Linux 内核版本范围：2017 年～修复补丁发布前

具体包括但不限于：

Ubuntu24.04LTS 及更早版本

Debian12、13 及更早版本

RHEL14.3 及更早版本

SUSE16 及更早版本

Amazon Linux2023 及更早版本

其他所有 2017 年后发布的主流 Linux 发行版（包括 Fedora、Arch、Rocky、Alma、Oracle Linux 等）

截止目前，绝大多数未更新至最新内核的生产系统均处于受影响范围。

2.威胁严重性

该漏洞可被本地普通用户 100%稳定利用，获取完整 root 权限，且已被公开 PoC 利用代码。考虑到该漏洞自 2017 年以来潜伏近十年，影响范围覆盖全球几乎所有 Linux 服务器，综合评估安全风险为高危。对校园网环境而言，多用户共享的计算节点、实验服务器、开发测试环境均面临直接威胁，建议按最高优先级进行应急处置。

四、处置建议

1.官方修复方案（推荐）

立即升级 Linux 内核至包含修复补丁的最新版本。

各主流 Linux 发行版已开始推送包含修复补丁（commit a664bf3d603d）的内核版本，请各单位根据所使用的操作系统类型执行相应操作：

- Ubuntu/Debian 系统：执行 sudo apt update && sudo apt upgrade linux-image-generic，然后重启系统
- RHEL/CentOS/Rocky/Alma 系统：执行 sudo yum update kernel 或 sudo dnf update kernel，然后重启系统
- SUSE 系统：执行 sudo zypper update kernel-default，然后重启系统

注：升级完必须重启才能生效。重启会导致业务服务短暂中断，请自行评估业务影响，选择合适的时间窗口进行升级和重启操作。如果暂时无法重启和升级，可以参考下面的临时方案。

2.临时缓解措施

若无法立即重启系统进行内核升级，可采用以下临时缓解措施——禁用受影响的 algif_aead 内核模块：

一键执行命令（需要 root 权限）：

echo "install algif_aead /bin/false" | sudo tee /etc/modprobe.d/disable-algif.conf && sudo rmmod algif_aead 2>/dev/null

执行完成后，可通过命令 lsmod | grep algif_aead 检查——如果没有输出，说明已成功禁用。

该临时措施无需重启系统即可生效。但请注意：禁用该模块可能影响依赖于 AF_ALG AEAD 加密功能的应用程序，请在操作前评估业务影响。