网络安全预警通报

2026 年第 5 期（总第 63 期）

西安交通大学网络信息中心 2026 年 05 月 09 日

【预警类型】高危预警

【预警内容】

Linux 内核 Dirty Frag 通用本地权限提升漏洞（QVD-2026-24699/CVE-2026-43284）高危风险通报

一、漏洞概述

近期，业界紧急披露了 Linux 内核中一个具有广泛影响的高危通用本地权限提升漏洞——Dirty Frag。该漏洞由安全研究员 Hyunwoo Kim（@v4bel）发现并公开，属于 Dirty Pipe 家族的衍生漏洞。

漏洞源于 Linux 内核 xfrm-ESP（ESP 协议处理）和 RxRPC（AFS 分布式网络文件系统协议）两个子系统的逻辑缺陷，在内核零拷贝路径（如 splice 系统调用）中对页面缓存（Page-Cache）进行不安全的内存就地加密处理，导致普通本地无特权用户可稳定利用此漏洞提升至 root 最高权限。

该漏洞具有高成功率（确定性逻辑漏洞，无需依赖复杂的竞争条件，利用失败不会导致内核崩溃）、跨发行版兼容性强、影响周期长（核心缺陷已潜伏长达约 9 年）、绕过已有漏洞缓解措施等特点。目前，官方完整补丁尚未发布，漏洞利用代码已经于 2026 年 5 月 7 日公开，建议各单位和用户按最高优先级立即开展排查与防护。

二、漏洞详情

1.技术原理

漏洞编号　QVD-2026-24699/CVE-2026-43284

漏洞名称　Linux Kernel Dirty Frag 本地权限提升漏洞

漏洞类型　本地权限提升（LPE）、通用逻辑漏洞

漏洞等级　高危

公开日期　2026 年 5 月 7 日

CVSS 3.1 评分　7.8

产生原因：

该漏洞可拆解为两个独立且可互补利用的子漏洞：

xfrm-ESP 页面缓存写入漏洞：自 2017 年 1 月 17 日起（commit cac2661c53f3）引入，攻击者可以利用用户命名空间权限，通过 splice 等零拷贝系统调用，将只读页面缓存页面插入网络缓冲区中，ESP 协议模块进行不安全的内存就地解包/解密操作，可实现对系统关键文件的内存副本进行任意 4 字节篡改。

RxRPC 页面缓存写入漏洞：自 2023 年 6 月（commit 2dc334f1a63a）起引入，无需任何特权（Ubuntu 等主流发行版默认加载 RxRPC 模块），

攻击者可利用该漏洞暴力破解加密密钥后篡改/etc/passwd 等配置文件，进一步删除 root 密码或直接提升权限。

值得注意的是，该漏洞不受此前 Copy Fail 漏洞（CVE-2026-31431）的 algif_aead 模块黑名单缓解措施的限制，已按此思路进行过加固的系统仍然存在严重安全风险。

2.利用条件

- 攻击者需要获得目标系统的本地普通用户权限（例如通过已被攻陷的 Web 服务、容器环境或已植入的恶意软件等）
- 目系统内核版本受上述漏洞影响（见下文受影响版本）
- 若要利用 xfrm-ESP 漏洞，依赖系统启用用户命名空间（unprivileged user namespace）；在容器环境中或在多数主流发行版中均默认启用或易于利用。
- 若要利用 RxRPC 漏洞，依赖系统加载 rxrpc.ko 内核模块（Ubuntu 等发行版默认加载，RHEL 等默认不加载，二者形成互补利用链）

三、漏洞影响范围

1. 受影响版本

xfrm-ESP 页面缓存写入漏洞：影响内核范围从 2017 年 1 月 17 日（commit cac2661c53f3）起，至上游最新版本。

RxRPC 页面缓存写入漏洞：影响内核范围从 2023 年 6 月（commit 2dc334f1a63a）起，至上游最新版本。

目前已确认受影响的主流 Linux 发行版包括但不限于：

Ubuntu 24.04.4（内核 6.17.0-23-generic）

RHEL 10.1（内核 6.12.0-124.49.1.el10_1.x86_64）

openSUSE Tumbleweed（内核 7.0.2-1-default）

CentOS Stream 10（内核 6.12.0-224.el10.x86_64）

AlmaLinux 10（内核 6.12.0-124.52.3.el10_1.x86_64）

Fedora 44（内核 6.19.14-300.fc44.x86_64）

以及各主流发行版的更早与更新版本均受此漏洞影响。

2.威胁严重性

该漏洞属于确定性本地提权漏洞，利用无需依赖竞争条件，不需要精确的时间窗口，攻击成功率接近 100%，且利用失败不会导致内核崩溃及系统不稳定，具有极高的隐秘性和可利用性。

一旦利用成功，攻击者可以获得完整的 root 最高权限，能够：

任意篡改系统关键配置文件（如/etc/passwd、/etc/sudoers），增加后门账户或直接删除管理员口令；

修改特权可执行文件的内存副本（如/usr/bin/su），绕过 PAM 认证流程直接获取 root Shell；

在主机上植入持久化后门/Rootkit，完全控制目标服务器；

在容器场景下，实现容器逃逸，影响底层宿主机乃至整个节点集群安全。

此漏洞与已被积极在野利用的 Copy Fail 漏洞属于同类型逻辑缺陷，而 Dirty Frag 影响的组件更为底层，覆盖范围更广，并且绕过了 Copy Fail 现有的缓解措施。

在校园网络环境和数据中心集群中，任何能够获取本地低权限 Shell 的入口（如被攻陷的 Web 应用、学生/教师个人计算节点、超算集群登录节点、容器镜像构建平台等）均可能成为攻击者利用此漏洞进行提权的跳板，须高度警惕。

四、处置建议

1.官方修复方案

截至本通报发布时，各主流 Linux 发行版官方尚未发布完整的内核补丁，安全补丁仍在开发与合并中。强烈建议用户持续关注各发行版安全公告，并及时更新系统内核。

2.临时的紧急缓解方案（建议根据自身系统情况自己决定）

禁用存在漏洞的 esp4、esp6 及 rxrpc 内核模块是目前最有效的临时防护手段。请以 root 或 sudo 权限执行如下命令（此操作将禁用 IPsec VPN 和 AFS 分布式文件系统功能，在实际使用中请根据业务需要酌情考虑）：

```
sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n'
> /etc/modprobe.d/dirtyfrag.conf; rmmod esp4 esp6 rxrpc 2>/dev/null; true"
```

执行后请通过 lsmod | grep -E "esp4|esp6|rxrpc"检查模块是否已成功卸载。若仍有残留模块，建议重启系统以确保该缓解措施全面生效。