网络安全预警通报

2026 年第 11 期（总第 69 期）

西安交通大学网络信息中心 2026 年 11 月 4 日

【预警类型】严重预警

【预警内容】

Linux 内核 IPv4 TCP 高危漏洞安全预警通报

一、病毒概述

近日，Linux 内核安全团队公开披露一个 Linux 内核 IPv4 TCP 网络协议栈高危安全漏洞，漏洞编号为 CVE-2026-98432。该漏洞属于 Use-After-Free（UAF，释放后使用）内存安全漏洞，主要存在于 Linux 内核 IPv4 TCP 连接处理过程中。攻击者在特定条件下，可通过远程构造 TCP 网络请求触发内存释放竞争，导致内核内存破坏、系统崩溃，甚至可能实现远程代码执行。

根据 Linux 内核官方公告，该漏洞影响范围可追溯至 Linux Kernel 4.4 版本，CVSS 3.1 评分为 9.8 分，威胁等级为严重（Critical）。漏洞利用无需身份认证，也无需用户交互。Anthropic 安全研究团队已展示利用该漏洞攻击启用 MPTCP 监听器的 Linux 服务器并获取

Root 权限的能力，表明该漏洞在特定配置下具有较高的实际攻击风险。

该漏洞主要与 Linux 内核处理 IPv4 TCP 连接请求时的内存生命周期管理有关。在 TCP 连接建立及重传过程中，不同 CPU 核心可能并发访问同一请求套接字关联的 IP 选项数据。当其中一个执行路径提前释放相关内存，而另一个执行路径仍继续访问该内存时，就可能触发 UAF 漏洞。

二、病毒详情

1.技术原理

CVE-2026-98432 是 Linux 内核 IPv4 TCP 网络处理模块中的 Use-After-Free 漏洞，主要涉及 TCP 连接请求处理及 Socket 迁移过程中相关内存对象的释放与访问竞争。

正常情况下，Linux 内核在处理 TCP 连接请求时，会创建请求套接字（Request Socket），用于保存连接建立过程中所需的信息，其中包括 IP 选项数据。

漏洞发生时，tcp_v4_syn_recv_sock()会将请求套接字中的 ireq_opt 所有权转移至新创建的子 Socket，但未对相关数据进行复制。与此同时，其他 CPU 核心可能正在处理同一连接请求的 SYN 重传，并继续读取原有 IP 选项数据。

当其中一个执行路径提前释放相关内存，而另一个执行路径仍然访问该内存时，就会形成释放后使用问题，进而造成内核内存访问异常。

Linux 内核官方针对该问题采用 kfree_rcu()替代原有的普通内存释放方式 kfree()，通过 RCU（Read-Copy-Update）机制延迟释放相关内存，确保其他 CPU 完成读取操作后再释放数据，从而解决相关内存竞争问题。

2.涉及病毒详情

漏洞名称：Linux 内核 IPv4 TCP Use-After-Free 漏洞

漏洞编号：CVE-2026-98432

漏洞类型：Use-After-Free（UAF，释放后使用）

漏洞组件：Linux Kernel IPv4 TCP 网络协议栈

CVSS 评分：9.8（CVSS 3.1）

威胁等级：严重（Critical）

影响版本：Linux Kernel 4.4 及后续受影响版本

攻击方式：远程网络攻击、TCP 连接请求竞争

身份认证：无需认证

用户交互：无需用户交互

主要危害：内核内存破坏、拒绝服务、潜在远程代码执行及 Root 权限获取

修复方式：升级至包含 CVE-2026-98432 修复补丁的 Linux 内核版本

主要修复机制：通过 kfree_rcu()延迟释放相关内存，避免并发访问已释放内存。

Linux 内核官方公布的主要修复版本如下：

内核分支　修复版本

5.10　5.10.272

5.155.15.223

6.1 6.1.190

6.6 6.6.159

6.126.12.113

6.186.18.56

7.2 7.2.10

7.3 7.3

以上为 Linux 内核上游公布的修复版本。不同 Linux 发行版可能采用补丁回移方式进行修复，实际修复情况应以各发行版官方安全公告及软件包版本为准，不能仅依据内核版本号判断是否存在漏洞。

3、主要识别特征

根据公开披露的信息，发现以下情况时应提高警惕：

（1）Linux 服务器运行的内核版本低于对应发行版公布的修复版本，且未确认是否已安装相关安全补丁。

（2）服务器对外开放 SSH、Web、数据库及其他 IPv4 TCP 服务，存在来自互联网或不可信网络的访问入口。

（3）服务器启用了 Multipath TCP（MPTCP），存在 MPTCP 监听 Socket 或相关连接迁移配置。

（4）服务器存在 net.ipv4.tcp_migrate_req 参数启用，或部署了与 Socket 迁移相关的 eBPF 程序等配置。

（5）系统运行过程中出现异常内核日志、内核崩溃、服务异常退出或非正常重启等情况。

（6）服务器尚未安装对应发行版提供的修复内核，或已安装新内核但未重启，当前运行的内核仍为存在风险的旧版本。

三、漏洞影响范围

1.影响范围

目前确认风险主要涉及：

- 使用 Linux Kernel 4.4 及后续受影响内核版本的服务器；
- 使用 Red Hat Enterprise Linux（RHEL）8、9、10 的服务器；
- 使用 Ubuntu 22.04、24.04 等版本的 Linux 服务器；
- 使用 Debian 12、Debian 13 等版本的 Linux 服务器；
- 使用 Amazon Linux 2、Amazon Linux 2023 的云服务器；
- 使用 Rocky Linux、AlmaLinux 等基于 RHEL 生态的 Linux 发行版，需结合各自官方安全公告确认修复情况；
- 部署 Web 服务、数据库服务、OA 系统及其他业务应用的 Linux 服务器；
- 对互联网开放 IPv4 TCP 访问端口的服务器；
- 启用了 MPTCP 监听服务的 Linux 服务器；
- 启用了 TCP Socket 迁移功能或部署相关 eBPF 程序的服务器；
- 使用 Linux 内核作为底层运行环境的容器节点、云计算平台及相关基础设施。

截至 2026 年 11 月 4 日，各发行版公开修复进展如下：

（1）Red Hat Enterprise Linux： RHEL 8、RHEL 9、RHEL 10 及 OpenShift Container Platform 均受到影响。截至 11 月 3 日，Red Hat 官方安全通报仍将相关漏洞标记为持续处理中，建议用户关注官方修复公告。

（2）Ubuntu： Ubuntu 22.04、24.04 的修复版本已进入-proposed 测试仓库，尚需关注正式更新仓库的发布情况；Ubuntu 26.10 已在 7.3.0-10.10 版本中修复，较早的受支持版本仍需关注后续安全更新。

（3）Debian： Debian 12、Debian 13 已发布对应修复软件包，主要修复版本分别为 6.1.190-1 和 6.12.113-1，实际安装情况应以官方安全跟踪系统为准。

（4）Amazon Linux： Amazon Linux 2 及 Amazon Linux 2023 已提供相关修复内核软件包，用户需要及时更新内核并重启服务器，使修复补丁生效。

需要注意的是，该漏洞并非仅在启用 MPTCP 的情况下才会受到影响。MPTCP 只是已公开展示的利用场景之一，漏洞本身涉及 IPv4 TCP 网络协议栈，因此单独关闭 MPTCP 不能作为完整的安全修复措施。对于尚未获得修复补丁的服务器，应重点加强网络访问控制，并持续跟踪发行版官方安全公告。

2.威胁严重性

攻击成功后，可能造成以下安全影响：

（1）远程获取服务器控制权限

攻击者在满足特定利用条件的情况下，可能利用内核内存竞争漏洞实现远程代码执行，进一步获取服务器 Root 权限，对服务器实施未授权操作。

（2）服务器系统崩溃

漏洞触发后可能造成内核内存访问异常，导致系统崩溃、异常重启或关键服务中断，影响服务器正常运行。

（3）内核内存数据遭到破坏

攻击者可能利用释放后使用问题破坏内核内存数据，影响系统运行稳定性，并可能进一步引发内存信息泄露等安全问题。

（4）业务系统运行受到影响

当运行数据库、Web 服务、OA 办公系统及其他重要业务应用的 Linux 服务器受到攻击时，可能导致业务服务不可用、数据访问异常及业务中断。

（5）服务器及内部网络安全受到威胁

如果攻击者通过漏洞获取服务器 Root 权限，可能进一步窃取业务数据、植入恶意程序、创建隐藏账号或利用服务器访问内部网络，扩大安全事件影响范围。

四、处置建议

1.及时开展资产排查。 全面梳理单位 Linux 服务器资产，重点核查操作系统发行版、内核版本及补丁安装情况，优先排查对互联网开放 IPv4 TCP 服务的服务器，确认是否存在 CVE-2026-98432 漏洞风险。

2.及时安装安全补丁。 根据服务器实际使用的 Linux 发行版，关注 Linux 内核官方及各发行版安全公告，及时安装包含 CVE-2026-98432 修复补丁的内核版本。更新完成后，应按照业务维护计划重启服务器，并通过 uname -r 确认当前实际运行的内核版本，确保修复补丁生效。

3.加强网络访问控制。 对暂时无法升级内核的服务器，应限制不必要的 IPv4 TCP 端口对外开放，通过防火墙等措施限制非可信来源访问。Red Hat 官方建议可评估过滤携带 IPv4 IP Options 的 TCP 数据包，以降低漏洞暴露风险，但相关规则需要结合实际网络环境进行测试，避免影响正常业务。

4.排查相关网络配置。 检查服务器 MPTCP 启用情况、TCP Socket 迁移配置及相关 eBPF 程序，重点关注 net.ipv4.tcp_migrate_req 参数和 MPTCP 监听服务。需要注意，关闭 MPTCP 不能彻底消除漏洞风险，不能替代内核安全补丁升级。

5.加强安全监测与应急处置。 持续关注服务器异常登录、异常进程、内核崩溃及系统异常重启等情况。发现疑似漏洞利用行为时，应及时开展日志分析、网络排查及应急处置，必要时隔离受影响主机，防止攻击者进一步扩大影响范围。