Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# One Script, Every Distro, Full Root: Copy Fail Vulnerability Rewriting Linux Threat Models


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| May 04, 2026 | A1 | TA2026119 |

# Summary

**First Seen:** March 23, 2026
**Affected Products:** Linux kernel (versions shipped from 2017 through 6.18.21 and 6.19.11), Ubuntu (including 24.04 LTS), Amazon Linux 2023, Red Hat Enterprise Linux (including RHEL 10.1), SUSE 16, Debian, Fedora, Arch Linux, AlmaLinux, CloudLinux, Oracle Linux, Rocky Linux, CentOS, and Kubernetes/Docker/LXC container hosts running affected kernels
**Impact:** The Copy Fail (CVE-2026-31431) vulnerability poses a critical risk to organizations operating Linux workloads at scale, particularly in cloud, container, CI/CD, and Kubernetes environments where untrusted code execution is routine. Successful exploitation results in full root privilege escalation, with high impact on confidentiality, integrity, and availability. Organizations whose isolation strategy depends on shared-kernel containers without microVM, gVisor, or dedicated-host boundaries should treat any container compromise as a potential host compromise. The combination of broad applicability across distributions, cross-architecture reliability, deterministic exploitation without race conditions, a sub-kilobyte exploit footprint, and a public proof-of-concept makes this one of the most impactful Linux kernel vulnerabilities.

## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-31431 | Copy Fail Vulnerability (Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability) | Linux Kernel | ✗ | ✓ | ✓ |

# Vulnerability Details

**#1**

Copy Fail (CVE-2026-31431) is a high-severity local privilege escalation flaw in the Linux kernel's cryptographic subsystem specifically a logic defect within the algif_aead module of the AF_ALG userspace crypto API. The bug allows any unprivileged local user to gain root on essentially every major Linux distribution shipped since 2017, including Ubuntu, Amazon Linux, Red Hat Enterprise Linux, SUSE, Debian, Fedora, Arch Linux, and downstream rebuilds such as AlmaLinux, CloudLinux, Oracle Linux, and Rocky Linux.

**#2**

A compact 732-byte Python proof-of-concept performs a controlled four-byte write into the kernel's in-memory page cache of any readable file setuid binaries such as /usr/bin/su being the obvious target. Because the modification never touches disk and the page is never marked dirty for writeback, file-integrity tools that rely on on-disk checksums miss it entirely, while the next invocation of the corrupted binary executes attacker-supplied shellcode and yields a root shell. Although no named threat actor has been linked to in-the-wild exploitation, Go and Rust ports of the original Python PoC have already surfaced in open-source repositories, signaling rapid weaponization.

**#3**

The flaw resides in authencesn, an AEAD (Authenticated Encryption with Associated Data) wrapper used by IPsec for 64-bit Extended Sequence Numbers. It is the cumulative product of three individually benign changes spread over six years: the 2011 authencesn implementation that repurposed the caller's destination buffer as scratch space for ESN byte rearrangement; a 2015 migration to the new AEAD interface that quietly introduced an out-of-bounds write at offset assoclen + cryptlen; and a 2017 in-place optimization to algif_aead.c (commit 72548b093ee3) that chained page-cache pages from splice() into the writable destination scatterlist. None of these commits was unsafe in isolation, which is precisely why the resulting vulnerability went undetected for almost a decade.

**#4**

The published exploit has been validated against Ubuntu 24.04 LTS (6.17.0-1007-aws), Amazon Linux 2023 (6.18.8-9.213.amzn2023), RHEL 10.1 (6.12.0-124.45.1.el10_1), and SUSE 16 (6.12.0-160000.9-default). The same binary runs unmodified across distributions and architectures no per-distro offsets, no recompilation, no version checks. Because exploitation requires no root inside a container, no kernel modules, and no network access, it slots cleanly into virtually any post-exploitation scenario: a compromised CI runner, a hijacked web container, or any unprivileged foothold on a multi-tenant host.

## Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2026-31431 | Linux Kernel versions shipped from 2017 through 6.18.21 and 6.19.11; fixed in 6.18.22, 6.19.12, and 7.0) | cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* | CWE-669 |

# Recommendations

**Apply Vendor Kernel Updates Immediately:** Update to a patched Linux kernel as the primary remediation. The upstream fix (mainline commit a664bf3d603d) reverts the algif_aead in-place optimization and is included in Linux kernel versions 6.18.22, 6.19.12, and 7.0. Distribution-specific fixed kernels are available from CloudLinux (kernel-4.18.0-553.121.1 for CL7h/CL8, kernel-5.14.0-611.49.2.el9_7 for CL9, kernel-6.12.0-124.52.2.el10_1 for CL10), AlmaLinux, Ubuntu, Amazon Linux, Red Hat, and SUSE through their normal kernel package update channels. Reboot is required after updating; Federal Civilian Executive Branch agencies have been mandated by CISA to apply fixes by May 15, 2026.

**Apply Live Kernel Patching Where Available:** Organizations that cannot tolerate immediate reboots should deploy live kernel patching solutions such as KernelCare, which has released CVE-2026-31431 livepatches to its main feed for AlmaLinux 8/9, CloudLinux 7h/8, CentOS 8, RHEL 8/9, Rocky Linux 8/9, Oracle Linux 7/8/9 (including UEK6), Proxmox VE 7, Ubuntu Bionic/Focal/Jammy (including AWS and Azure variants), Debian 11/12, and equivalents. Subscribed systems receive the fix automatically on the next kcarectl --update invocation, with verification via kcarectl --info | grep CVE-2026-31431.

**Apply Interim Mitigations If Patching Is Delayed:** Where immediate patching is not possible, block AF_ALG AEAD interface registration at boot using the kernel command-line parameter initcall_blacklist=algif_aead_init applied via grubby and a reboot. This closes the attack surface without replacing the kernel and can be reverted in seconds once a patched kernel is installed. The modprobe-based workaround (install algif_aead /bin/false) circulating on oss-security does not work on RHEL-family distributions because algif_aead is built into the kernel (CONFIG_CRYPTO_USER_API_AEAD=y) rather than loaded as a module. Compatibility analysis confirms that dm-crypt/LUKS, kTLS, IPsec, SSH, and default OpenSSL/GnuTLS builds do not depend on AF_ALG and are unaffected by this mitigation; only applications explicitly using AF_ALG for AEAD ciphers (such as OpenSSL with the afalg engine enabled or AF_ALG-based hardware crypto offload) will be impacted.

**Strengthen Container and Multi-Tenant Isolation Boundaries:** Treat any container remote code execution incident on a vulnerable kernel as a potential host compromise and enforce rapid node recycling after compromise indicators are observed. Because the Linux page cache is shared between containers and the host, namespace-based isolation does not contain Copy Fail. For workloads executing untrusted code (multi-tenant Kubernetes clusters, CI/CD runners accepting pull requests from forks, and AI agent code-execution sandboxes), evaluate migration to hardware-or-VM isolation boundaries such as Firecracker microVMs, gVisor user-space kernels, or dedicated-host configurations that do not share a Linux kernel across tenants.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Discovery | T1082: System Information Discovery | |
| Execution | T1059: Command and Scripting Interpreter | T1059.006: Python |
| Privilege Escalation | T1068: Exploitation for Privilege Escalation | |
| | T1611: Escape to Host | |
| Defense Evasion | T1564: Hide Artifacts | |

## Patch Link

https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=893d22e0135fa394db81df88697fba6032747667

## References

https://www.microsoft.com/en-us/security/blog/2026/05/01/cve-2026-31431-copy-fail-vulnerability-enables-linux-root-privilege-escalation/

https://xint.io/blog/copy-fail-linux-distributions

https://www.sophos.com/en-us/blog/proof-of-concept-exploit-available-for-linux-copy-fail-cve-2026-31431

https://www.forbes.com/sites/daveywinder/2026/05/03/update-linux-now-as-9-year-old-root-hack-confirmed-cisa-warns-users/

https://www.hkcert.org/security-bulletin/linux-kernel-elevation-of-privilege-vulnerability_20260504

https://blog.cloudlinux.com/cve-2026-31431-copy-fail-kernel-update

https://www.wiz.io/blog/copyfail-cve-2026-31431-linux-privilege-escalation-vulnerability

https://socprime.com/active-threats/cve-2026-31431-copy-fail-linux-root-escalation/

https://securelist.com/tr/copyfail-root-linux/119634/

https://copy.fail/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

**May 04, 2026 • 06:00 AM**



More at www.hivepro.com