Linux Kernel "Copy Fail" Privilege Escalation Vulnerability Actively Exploited

TL;DR

A Linux kernel vulnerability (CVE-2026-31431, CVSS pending) is now being actively exploited. The flaw allows a local, unprivileged user to gain root access on affected systems. It impacts most Linux distributions released since 2017.

A public proof-of-concept exploit is already available and works reliably across multiple environments. Organizations should patch immediately and treat exposed systems as compromised.

Overview

There is a privilege escalation vulnerability in the Linux kernel (CVE-2026-31431, CVSS pending) that is now being exploited in the wild. The issue is in the algif_aead cryptographic interface and allows a local user to write controlled data into the page cache of readable files.

Affected Products

- Linux kernel versions built between 2017 and the patched release (varies by vendor)
- Confirmed impacted distributions include:
  - Ubuntu 24.04 LTS
  - Amazon Linux 2023
  - Red Hat Enterprise Linux 10.1
  - SUSE Linux 16

Once triggered, this behavior can be abused to gain root-level access on the system. The exploit does not require special conditions like race timing or kernel offsets. It works in a straightforward and repeatable way, which lowers the barrier for attackers.

There is confirmation that the exploit works across major distributions including Ubuntu, Amazon Linux, Red Hat Enterprise Linux, and SUSE. The same exploit code functions across environments without modification, which increases the risk for organizations running mixed Linux environments.

The vulnerability affects kernels built between 2017 and the patched versions, meaning most modern Linux systems are exposed if not updated. The Cybersecurity and Infrastructure Security Agency (CISA) added this vulnerability to its Known Exploited Vulnerabilities (KEV) catalog and directed federal agencies to patch by May 15, 2026.

Aspire Protects

- **Patch** - Organizations should update the Linux kernel through their operating system's standard update process. Because this vulnerability affects the kernel itself, applying the patch requires installing a vendor-provided kernel update and rebooting the system.
    - Identify all Linux systems in your environment - servers, cloud instances, containers, and CI/CD runners.
    - Check the current kernel version using `uname -r`
    - Apply vendor updates using your system package manager:
        - Ubuntu / Debian - `apt update && apt upgrade -y`
        - Red Hat Enterprise Linux / Amazon Linux - `dnf update -y` (or `yum update -y` for older systems)
        - SUSE - `zypper update -y`
    - Reboot systems after updating - the new kernel does not take effect until reboot.
    - Verify the patch after reboot by running `uname -r` and confirming the system is on a patched kernel version.
    - Prioritize high-risk systems first - multi-user servers, Kubernetes nodes, CI/CD runners, and environments running untrusted code.
    - If patching is delayed, temporarily disable the vulnerable module:
        - `echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif.conf`
        - `rmmod algif_aead`
- Monitor for privilege escalation activity - Watch for unusual root-level process creation or user escalation events.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit a kernel vulnerability to gain root-level access on the system.

Defense Evasion

- Modify System Image [T1601] – The attacker may manipulate memory structures such as the page cache to alter system behavior without modifying files on disk.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This vulnerability impacts any organization running Linux systems, especially environments with shared access or user-executed workloads:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Copy Fail — CVE-2026-31431

Will Dormann: "While this vulnerability seems…" - Infosec Exchange

Copy Fail: 732 Bytes to Root on Every Major Linux Distribution. - Xint