CERT-EU

Security Advisory 2026-005

High Vulnerability in the Linux Kernel ("Copy Fail")

2026-04-30 — v1.0

TLP:CLEAR

History:

- *29/04/2026 — v1.0 – Initial publication*

Summary

On 29 April 2026, a high local privilege escalation vulnerability in the Linux kernel, tracked as **CVE-2026-31431** and named **"Copy Fail"**, was publicly disclosed [1].

The vulnerability affects every mainstream Linux distributions shipping a kernel built since 2017. A public proof-of-concept exploit has been released.

As of the date of this advisory, **no distribution has shipped a fixed kernel package**. The mainline fix was committed on 1 April 2026, but vendor updates are still pending across all major distributions. CERT-EU strongly recommends applying the interim mitigation immediately, prioritising Kubernetes nodes, and CI/CD runners exposed to untrusted workloads.

Technical Details

The vulnerability **CVE-2026-31431**, with a CVSS score of 7.8, is a local privilege escalation flaw in the Linux kernel's `algif_aead` module, the AEAD socket interface of the kernel's userspace crypto API (`AF_ALG`). The flaw originates from an in-place optimisation introduced in 2017 (commit `72548b093ee3`), which allows page-cache pages to be placed into a writable destination scatterlist. By chaining an `AF_ALG` socket operation with `splice()`, an unprivileged local user can perform a controlled 4-byte write to an arbitrary page-cache-backed page, targeting a setuid binary such as `/usr/bin/su` to obtain a root shell [1].

The upstream fix is mainline commit `a664bf3d603d`, which reverts the 2017 optimisation. It was committed on 1 April 2026 [1].

Affected Products

The vulnerability affects every mainstream Linux distribution shipping a kernel built between 2017 and the availability of the patch. The following distributions were directly verified by the researchers [1]:

Distribution	Kernel Version
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
SUSE 16	6.12.0-160000.9-default

Other distributions running kernels in the affected range are implicitly affected, including Debian, Arch Linux, Fedora, Rocky Linux, AlmaLinux, Oracle Linux, and embedded Linux distributions.

Patch availability by distribution (as of 30 April 2026):

Distribution	Status
Ubuntu 20.04–24.04	No fix available
Amazon Linux 2023	No fix available
SUSE Linux Enterprise	No fix available
Red Hat Enterprise Linux	Status unknown

Note: Ubuntu 26.04 (Resolute) and later kernels are **not affected** [2].

Additional information is available in the researcher's advisory [1] and in vendor security trackers [2,3,4].

Recommendations

CERT-EU strongly recommends applying the relevant kernel update as soon as possible once vendor patches become available, prioritising Kubernetes nodes and CI/CD runners.

Temporary Mitigation

Disable the `algif_aead` kernel module persistently on all affected systems until a patched kernel is available:

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

This workaround does not affect `dm-crypt`/LUKS, `kTLS`, IPsec/XFRM, OpenSSL, GnuTLS, NSS, or SSH. It may affect applications explicitly configured to use the `afalg` engine or that bind `aead`/`skcipher`/`hash` sockets directly. Exposure can be assessed with `lsof | grep AF_ALG`.

Hardening Containerised Environments and Pipelines

CERT-EU recommends blocking `AF_ALG` socket creation via seccomp policies on all containerised workloads and pipelines, regardless of patch status [1]. This applies to Docker and Podman-based environments [5] as well as Kubernetes clusters [6]. Since the exploit requires opening an

`AF_ALG` socket as a first step, this measure effectively prevents exploitation even on unpatched kernels.

References

[1] https://copy.fail

[2] https://ubuntu.com/security/CVE-2026-31431

[3] https://www.suse.com/security/cve/CVE-2026-31431

[4] https://access.redhat.com/security/cve/CVE-2026-31431

[5] https://docs.docker.com/engine/security/seccomp/

[6] https://kubernetes.io/docs/tutorials/security/seccomp/