

Forum:[Hack Forums](#)

Thread: [Linux in trouble, all distro from 2017 till 2026](#)

raw999 - May 2, 2026, 5:58 am

New Linux Exploit "Copy Fail" Gains Root Access on Almost Every Distro

A new Linux vulnerability just dropped — and it's one of the most serious ones in years.

It's called "Copy Fail" and it affects almost every major Linux distribution released since 2017

What Is "Copy Fail"?

Copy Fail is a local privilege escalation (LPE) vulnerability in the Linux kernel.

How the Exploit Works

Without going too deep:

1. Attacker uses a flaw in the Linux crypto API
2. Writes small controlled data into page cache
3. Targets a setuid binary (runs as root)
4. Modifies behavior in memory
5. Gains root access

Lablear - May 2, 2026, 11:28 am

Cough

> a simple update is insufficient without a full system reboot to flush the potentially corrupted page cache from RAM.

? loading encrypted image...

"The vulnerability resides within the algif_aead module of the AF_ALG interface.² AF_ALG is a socket-based interface introduced to allow userspace applications to access the kernel's internal cryptographic hardware and optimized software implementations.² It supports various types of cryptographic operations, including symmetric ciphers, hashes, and AEAD (Authenticated Encryption with Associated Data).²

In July 2017, commit 72548b093ee3 was merged into the mainline kernel to optimize AEAD operations in algif_aead.² The optimization introduced support for "in-place" operations, where the source buffer (containing the data to be encrypted or decrypted) and the destination buffer (where the result is stored) are the same physical memory.⁴ This was intended to reduce memory pressure and improve performance by avoiding unnecessary copies.¹²

The critical logical failure occurred when this in-place logic interacted with the splice() system call.⁴ splice() is an optimization that allows moving data between two file descriptors (like a file and a socket) without copying that data to userspace.⁴ When a user "splices" a file into an AF_ALG socket, the kernel creates a "scatterlist"—a series of pointers—that points directly to the file's pages in the page cache.⁴ By allowing "in-place" operations on these spliced pages, the kernel mistakenly

treated the read-only page cache as a writable destination buffer for the cryptographic operation.1"

Thanks, Had multiple LLM instances run to analyze your post and so far it's produced some fine material

HALx86 - May 2, 2026, 12:44 pm

This is pretty legit. I tested it on a few boxes today.

Make sure you have unattended-upgrades on and run your patches.

raw999 - May 2, 2026, 12:56 pm

I've transferd to ubuntu and updated, they seem to be only to patch it.
Or?

Lablear - May 2, 2026, 2:44 pm

for support and details head to <https://copy.fail/>