Copy Fail Linux Vulnerability (CVE-2026-31431)

Article Number: 2039 | Rating: 4.2/5 from 5 votes | Last Updated: Thu, Apr 30, 2026 at 10:19 AM

On 29 April 2026, security researchers at Theori (Xint Code) publicly disclosed CVE-2026-31431, known as "Copy Fail." It is a local privilege escalation flaw in the Linux kernel's AF_ALG cryptographic interface. Any unprivileged local user — including a compromised web application running as a low-privilege user such as www-data, apache, or a cPanel customer account — can escalate to root within seconds. The vulnerability has existed in mainstream Linux kernels since 2017 and a working public exploit is already in circulation. **Not affected by this vulnerability**: CentOS 5, 6, and 7 Ubuntu 14.04 and earlier Debian 8 and earlier **Note**: while these releases are not vulnerable to CVE-2026-31431, they are all end-of-life and no longer receive security updates. We strongly recommend migrating to a supported release. **Affected:** AlmaLinux, Rocky Linux, RHEL, CloudLinux (versions 8 and 9) CentOS 8 and CentOS Stream 8/9 Ubuntu (all currently supported releases: 20.04, 22.04, 24.04) Debian 9 and later CentOS 8 customers should note that CentOS 8 reached end of life on 31 December 2021 and no patched kernel will be released by the project. The mitigation in Step 2a will protect against this specific CVE, but migration to AlmaLinux 8 (a drop-in replacement) or a fresh AlmaLinux 9/10 build is strongly recommended. If you are unsure which distribution you are running, the following command will tell you: cat /etc/os-release **Step 1:** Confirm whether your kernel is vulnerable Run this command as root: grep CRYPTO_USER_API_AEAD /boot/config-$(uname -r) No output, or the file does not exist: your kernel is not affected. No further action required. Output ending in =m (typical for Ubuntu and Debian): affected, follow Path B below. Output ending in =y (typical for AlmaLinux, Rocky, RHEL, CloudLinux): affected, follow Path A below. **Step 2a (Path A):Â** AlmaLinux / Rocky / RHEL / CloudLinux On these distributions the vulnerable code is compiled directly into the kernel, so the standard module-blacklist approach will silently fail and leave your server vulnerable. Use the following kernel boot parameter instead, which prevents the vulnerable subsystem from initialising at boot: grubby --update-kernel=ALL --args="initcall_blacklist=algif_aead_init"
reboot *A reboot is required for the change to take effect.* **Step 2b (Path B):Â** Ubuntu / Debian --- On these distributions the vulnerable code is a loadable module and can be disabled with: echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif.conf
rmmod algif_aead 2>/dev/null || true A reboot is not strictly required but is recommended to ensure the configuration is loaded cleanly on next boot. **Step 3:** Verify the mitigation has taken effect As a non-root user, run the following test. It attempts to bind an AF_ALG AEAD socket — the operation an attacker would perform — and reports whether the kernel still permits it: perl -e '
use Socket;
socket(S, 38, 5, 0) or die "socket: $!";
my $addr = pack("S a14 L L a64", 38, "aead", 0, 0, "authenc(hmac(sha256),cbc(aes))");
bind(S, $addr) or die "bind: $!";
print "bind ok\n";
' Output "bind ok" — your server is still vulnerable. Re-check Step 2 and ensure you have rebooted (Path A) or run rmmod (Path B). Output "bind: No such file or directory" — the mitigation is working. Â **Step 4:** Apply the official kernel patch when available The mitigation above disables the AF_ALG authenticated-encryption interface. This is safe for the overwhelming majority of workloads — it is not used by SSH, OpenSSL, dm-crypt/LUKS, IPsec, or kTLS — but it should be considered a temporary measure. When your distribution publishes a kernel update incorporating upstream commit a664bf3d603d, please apply it and reboot: Ubuntu / Debian: apt update && apt upgrade && reboot AlmaLinux / Rocky: dnf update kernel && reboot CloudLinux: a kernel update and a KernelCare live patch are in active development. Please monitor https://cloudlinux.statuspage.io for availability. Once the patched kernel is running, the temporary mitigation can be removed if you wish. **Need assistance?** If you would prefer a Heart Internet engineer to apply the mitigation on your server, please raise a ticket through your control panel and reference â€œCVE-2026-31431â€• but please be aware that managed customers are being prioritised.

Posted - Thu, Apr 30, 2026 at 9:45 AM.

Online URL: https://www.heartinternet.uk/support/article/copy-fail-linux-vulnerability-cve-2026-31431.html