مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Local Privilege Escalation vulnerability in the Linux kernel

Tracking #:432318870

Date:01-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity local privilege escalation vulnerability, dubbed Copy Fail (CVE-2026-31431), has been disclosed in the Linux kernel's cryptographic subsystem.

TECHNICAL DETAILS:

A high-severity local privilege escalation vulnerability, dubbed Copy Fail (CVE-2026-31431), has been disclosed in the Linux kernel's cryptographic subsystem. The flaw allows an unprivileged local user to perform a controlled 4-byte write into the page cache of any readable file on the system, enabling modification of privileged binaries (such as setuid executables) in memory to achieve root access.

Vulnerability Details

- **CVE ID:** CVE-2026-31431
- **Nickname:** Copy Fail
- **CVSS Score:** 7.8 (High)
- **Vulnerability Type:** Local Privilege Escalation (LPE)
- **Affected Component:** Linux Kernel – Cryptographic subsystem (algif_aead interface)
- **Public Exploit**: Yes — A short, reliable Python PoC is available on GitHub.

Impact:

- Unprivileged local attacker can overwrite a few controlled bytes in the page cache of a setuid binary or other privileged file.
- Leads to reliable root shell execution.
- Changes are memory-only (page cache); they disappear on reboot or cache eviction, evading standard disk-based forensics.
- Can potentially cross container boundaries in shared kernel environments.

Affected Systems:

- Linux kernel versions 4.14 and later
- Virtually all major distributions released since 2017

Distribution Patch Status (as of April 30, 2026)

Fixed kernel versions include: 5.10.254, 5.15.204, 6.1.170, 6.6.137, 6.12.85, 6.18.22, and newer mainline releases.

- Ubuntu → Patching
- SUSE → Patching
- Red Hat → Patching
- Debian → Vulnerable
- Amazon Linux → Vulnerable
- Arch Linux → Patched

RECOMMENDATIONS:

- Immediate Actions: Apply vendor-provided kernel updates immediately.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2026-31431