Copy Fail Security Bulletin

Date: 2026-05-01

Summary

Viavi Solutions product teams are aware of the Copy Fail Linux vulnerability (CVE-2026-31431) and are currently assessing its impact across all NSE product lines.

While this is not a vulnerability in Viavi Solution's software, it has possible impact on the operating system on which many of our software products run.

Further details are expected early the week of May 3, 2026 and will be posted to this site when available. This will include product impact assessment and recommended mitigation actions where applicable.

Vulnerability Details

CVE-2026-31431, known as "Copy Fail," is a local privilege escalation (LPE) vulnerability in the Linux kernel's cryptographic template (algif_aead module). An unprivileged local user can trigger a deterministic, controlled 4-byte write into the page cache of any readable file on the system by chaining AF_ALG and splice() calls. By modifying the cached copy of a setuid binary, an attacker can alter the binary for the purpose of program execution and obtain root.

The vulnerability has been present since Linux kernel 4.14 (2017) and affects all major distributions, including Ubuntu, RHEL, Amazon Linux, and SUSE. It carries a CVSS v3.1 score of 7.8 (High). While not remotely exploitable on its own, it represents a container escape primitive on shared-kernel deployments because the page cache is shared across the host, and may be chained with a remote foothold (web RCE, malicious CI runner, or SSH compromise) for end-to-end compromise.

References

https://cert.europa.eu/publications/security-advisories/2026-005/

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