Linux Kernel Privilege Escalation Vulnerability (Copy Fail)

Date: 2026-06-11
Version: 1.0

Summary

A logic bug in the Linux kernel, known as “Copy Fail,” allows local attackers to gain root or administrator privileges. The attack is easy to carry out and goes undetected by common security scanners. This vulnerability affects Linux distributions using affected kernels released since 2017. We therefore recommend that you patch your servers as soon as possible.

The following vulnerability does not affect Connectivity Suite itself. It may affect the underlying Linux operating system on which the software is deployed. The operating system and its patching remain the responsibility of the system owner or operator and are not part of Belden’s product responsibility.

ID	Title / Description	Severity
CVE-2026-31431	Linux kernel local privilege escalation vulnerability (“Copy Fail”) allowing a local attacker to obtain root privileges on affected systems.	CVSS v3.1: 7.8 High

Affected Products

Brand	Product Line	Affected Version(s)
Belden	Connectivity Suite	Not directly affected; underlying customer-managed Linux operating system may be affected

Mitigation

Apply the latest vendor-supplied Linux kernel security updates and reboot affected systems to load the patched kernel. Prioritize internet-facing systems, shared servers, Kubernetes nodes, and CI/CD runners. If immediate patching is not possible, restrict local access and follow your Linux vendor’s interim mitigation guidance until the update can be installed.

For Help or Feedback

To view all Belden Security Advisories or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://www.belden.com/support/technical-product-support-main.

Related Links

- [1] NVD - CVE-2026-31431

Disclaimer

THE ADVISORY, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE ADVISORY, IS AT YOUR OWN RISK. INFORMATION IN THIS ADVISORY AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE ADVISORIES AT ANY TIME.

Revisions

V1.0 (2026-02-20) Security Advisory published.