Bizerba SE & Co. KG
Wilhelm-Kraut-Straße 65
72336 Balingen

Security Advisory

Privilege Escalation Vulnerability on all Linux Operating Systems since 2017 “Copy Fail”
CVE-2026-31431

1. Summary

   The crypto / subsystem in the Linux kernel has a severe logic bug allowing a standard user to get root privileges. This has been confirmed and a 732 bytes proof-of-concept python script exists.

   Bizerba was able to reproduce this on vulnerable Linux kernel versions. Additionally, Python and other interpreters and runtimes are available on most of the Bizerba scale products.

   Besides, an attacker needs:

   - a way to place malicious exploitation code on the system
   - a way to execute the code like an additional RCE vulnerability or for example access to the command line interface

   This adds a layer of complexity on top of the general CVSS score mentioned below.

2. Affected Products

Q1 pro	devices are not affected, the vulnerable kernel module is not built into the kernel itself
Q1 expert	Standard devices with Open Suse SlowRoll **are affected**
K3	Standard devices with Open Suse SlowRoll **are affected**
XC2 pro	Standard devices are not affected
KH II pro	Standard devices are not affected

3. Mitigation

   General short-term mitigation steps are described here:
   Copy Fail — CVE-2026-31431

   Customers are kindly informed that Bizerba doesn’t provide any warranty on directly applied fixes and product modification besides officially released vulnerability packages.

4. Solution

Information Protection Class - Public

Bizerba SE & Co. KG
Wilhelm-Kraut-Straße 65
72336 Balingen

Bizerba will provide vulnerability packages for the affected OpenSuse SlowRoll devices deactivating the affected kernel module algif_aead as a short-term solution.

These security patches only apply to the last two versions of scale software Retail Store (1.11, 1.12).

5. Technical Details

   The vulnerability “Copy Fail” (CVE-2026-31431) is based on a logic error inside the Linux kernel crypto-module “AF_ALG”. This crypto API allows socket connections from unprivileged processes to perform crypto operations.

   The exploit allows the injection of a malicious shell payload into the page cache of any binary allowing the user to effectively modify any binary script logic like “su” and finally starting the exploit by loading the tainted page cache.

6. CVSS Rating
   Base Score: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H&version=3.1
   Temporal Score: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C&version=3.1

7. References
   Sicherheitslücke Linux CVE-2026-31431 ("Copy Fail")
   New Linux ‘Copy Fail’ flaw gives hackers root on major distros
   „Copy Fail“: Linux-root in allen großen Distributionen mit 732 Byte Python | heise online
   Copy Fail — CVE-2026-31431
   How Cloudflare responded to the “Copy Fail” Linux vulnerability

8. Timeline

   Vulnerability packages are planned to be released mid to end of May 2026.