Security Advisory

Copy Fail CVE-2026-31431 - 08.05.2026 (v1.0)

Background

A local privilege escalation (LPE) vulnerability in the Linux kernel was publicly disclosed on April 29, 2026. The vulnerability has been assigned CVE-2026-31431 and is nicknamed “Copy Fail,” the vulnerability affects the Linux kernel’s algif_aead component within the AF_ALG cryptographic interface. Successful exploitation allows an unprivileged local user to gain root privileges on affected systems.

The vulnerability has a CVSSv3.1 score of 7.8 and is rated as HIGH severity.

Axis Response

Axis has been actively monitoring this vulnerability since the initial reports and immediately initiated an investigation to assess the potential impact on AXIS OS devices.

Our investigation has confirmed that certain products use Linux kernel versions affected by this vulnerability as part of their AXIS OS software.

To help keep systems secure, we are preparing updated AXIS OS releases for the following tracks:

- Active Track 12
- LTS 2024 11.11
- LTS 2022 10.12
- LTS 2020 9.80

It is recommended to update the Axis device software. The latest Axis device software can be found here. For further assistance and questions, please contact Axis Technical Support.

To reduce potential exposure, we recommend implementing the measures outlined in the AXIS OS hardening guide.

We will continue to closely monitor the situation and provide updates as additional information becomes available.

Axis Communications AB, Gränden 1, SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com