Initial Customer Communication

Security advisory: CVE-2026-31431 ("Copy Fail") — May 6, 2026

Status: Under investigation

Overview

Digi International is currently reviewing CVE-2026-31431 to determine whether any of our products and services are affected by this vulnerability. This advisory will be updated once our assessment is complete.

Impact summary

CVE-2026-31431, commonly referred to as "Copy Fail," is a local privilege escalation (LPE) vulnerability in the Linux kernel's algif_aead cryptographic module, disclosed on April 29, 2026.

Public sources indicate this vulnerability affects Linux kernel builds from 2017 onwards across multiple distributions, including Ubuntu, RHEL, Amazon Linux, and SUSE. An unprivileged local user may be able to exploit this issue to gain root-level access on affected systems.

Digi International’s Response

Our security and engineering teams have initiated a review of our products and services to determine exposure to this vulnerability. We are actively assessing which, if any, offerings incorporate the affected kernel component and will take remediation action where necessary as soon as possible. We will update this advisory as findings become available.

Customer guidance

At this time, we are not able to provide product-specific guidance while our investigation is ongoing. Customers should continue to follow general security best practices in their own environments, including:

- Applying the latest kernel security updates from your Linux vendor as soon as they are available and tested in your environment.
- Restricting unprivileged local user access on sensitive systems where possible.
- Monitoring systems for unexpected privilege changes or anomalous activity.

Contact information

For questions or concerns, customers may contact Digi International Customer Support or their designated account representative.

Status and updates

This advisory will be updated weekly as new information becomes available.