Security advisory: CVE-2026-31431 ("Copy Fail") — June 18, 2026 Update

Status: **Assessment complete**

Overview

Digi International has completed its review of CVE-2026-31431 across our products and services. The findings for each product family are detailed below. This page supersedes the initial advisory published on May 4, 2026.

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 products and services

Product category	Product / service	Status
MSBU (Cellular/Ventus)	Digi Accelerated Linux (DAL) — Digi EX/IX/TX Family	TX Family - vulnerable; patched in 26.2.148.158
		EX and IX Families - Not vulnerable
	Digi xOS	Not affected
	Digi Remote Manager (Digi RM)	Mitigated
	Digi On-Prem Manager (DOM)	Mitigated
	ARMT	Not affected
Particle/OEM (Embedded Systems)	ConnectCore Family	Patched; Patched in version DEY-5
	Digi Embedded Android	Not affected
	Digi HX15 Gateway Family	Not affected
	Digi HX20 Gateway Family	Not affected
	Digi XON	Not affected
	Older NDS/GeneOS products (ConnectPort X4, etc.)	Not affected

	Xbee Zigbee Wi-Fi Hub	Not affected
	Xbee Industrial Gateway	Not affected
	XBee 3 Cellular	Not affected
	XBee Gateway	Not affected
	XBee Hive	Patch released; Patched in version 26.4.41.25
	XBee Hive Border Router	Patch released; Patched in version 26.4.41.25
	XBee RF Family (long and short)	Not affected
	XBee SX / Wi-Sun / XR / XBee-PRO	Not affected
	Particle Embedded Devices	Not affected
	Particle Tachyon	Mitigated
	Particle Cloud	Mitigated
IM (Cellular/Networking)	Connect Sensor+ Family	Not affected
	Digi AnywhereUSB Manager	Not affected
	Digi AnywhereUSB Plus Family	Not affected
	Digi Axess	Mitigated
	Digi Connect EZ Family	Not affected
	Digi Connect IT Family	Not affected
	Digi ConnectPort LTS & TS Family	Not affected
	Digi Navigator	Not affected
	Digi PortServer Family	Not affected
	Digi Realport	Not affected
	Edgeport Family	Not affected
	Hubport Family	Not affected
	Z45 Industrial Controller Family	Not affected
Opengear	ACM7000 Resilience Gateway	Not affected
	CM7100 Console Server	Not affected
	CM8000, CM8100 Console Server	Mitigation; https://portal.opengear.com/customerservice/s/article/CVE-2026-31431-Linux-Kernel
	IM7200 Infrastructure Manager	Not affected
	OM1200, OM1300, OM2200 Operations Manager	Not affected
	Lighthouse	Patch released; https://ftp.opengear.com/download/lighthouse_software/all/26.04/current/
SmartSense	B2 Sensor	Not affected
	B3 Sensor	Not affected

	BZ Gateway	Not affected
	Cloud Dashboard	Patches in progress
	Jolt Products	Mitigated
	NIST Probes	Not affected
	Sensor Hub	Not affected
	Smart Shield	Not affected
	SmartLink	Not affected
	T1 Sensor	Not affected
	Z Sensor	Not affected
IT	Professional Services	Mitigated

Digi International's response

Our security and engineering teams have completed their review of Digi's products and services. Where affected components have been identified, remediation actions are being taken according to each product team's standard patching and release process. We will continue to update this advisory as fixes become available.

Customer guidance

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.

Customer guidance

Digi strongly recommends that customers running affected products update to the latest available firmware as soon as possible. Firmware updates containing the remediation for CVE-2026-31431 will be listed in the product table above as they become available.

To update your device firmware:

- Log in to your device management portal and use the firmware update feature to push the latest release to your devices.
- Alternatively, download the latest firmware directly from the product support page and apply it via your device's local management interface.

- If you are unsure which firmware version your device is running, refer to your product's user guide or contact Digi Customer Support.

In the interim, customers should restrict local user access on sensitive systems where possible and monitor for any unexpected privilege changes or anomalous activity on Linux-based Digi devices.

Status and updates

This advisory will be updated if new information becomes available.

Contact information

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