Copy Fail Security Bulletin

Date: 2026-05-04

Vulnerability Details

CVE-2026-31431, known as “Copy Fail,” is a local privilege escalation (LPE) vulnerability in the Linux kernel’s cryptographic template (algif_aead module).

The vulnerability has been present since Linux kernel 4.14 (2017) and affects all major distributions, including Ubuntu, RHEL, Amazon Linux, and SUSE. It carries a CVSS v3.1 score of 7.8 (High). While not remotely exploitable on its own, it represents a container escape primitive on shared-kernel deployments because the page cache is shared across the host, and may be chained with a remote foothold (web RCE, malicious CI runner, or SSH compromise) for end-to-end compromise.

Viavi Response

While this is not a vulnerability in Viavi Solution’s software, it does impact the OS on which many of our software products run.

For those impacted products, Viavi’s response is based on the product OS and commercial agreement around OS management:

Category	OS Supplier	Response
A	Viavi-provided	Viavi will reach out to customer contact in May to coordinate application of vulnerability mitigation.
B	Customer-provided	Customer is responsible to apply OS patching for vulnerability mitigation. Guidance provided below. For customers under SUS contract requiring support with solution restart, please raise support ticket via standard Support Portal channel.
C	Viavi SAAS	Viavi has already performed the required mitigations.

Risk Assessment

Below is a table of products affected and their planned remediation.

Viavi Business Unit	Viavi Products	Impacted	Viavi Response Category
NE - FAS	Fusion – server Fusion – virtual agent	True	A B
SE – WES	MNO	True	B
SE – AMS	NITRO Mobile Apps NITRO Mobile Probe NITRO DB w/ NITRO Mobile	True	A A A
SE – AMS	NITRO GEO NITRO LI NITRO DB w/ NITRO GEO	True	B
SE - AMS	NITRO AIOPs	True	B
SE – NPTS	GigaStore Apex	False	-
SE – NPTS	GigaFlow	True	A – appliance B – Virtual Machine
NE – L&P	TestCenter Lab Center	False	-
NE – L&P	TestCenter Windows App	False	-
NE – L&P	TestCenter - Linux Deployments	False	-
NE – WBU	Cyber Flood - Appliance	False	-
NE – WBU	Cyber Flood – Virtual	False	-
NE – WBU	Channel Emulation	False	-
NE - FAS	ONA 800, 1000 Platforms and all Metro Products(MTS 5800), ONXF, DCX	False	-
SE - AMS	NITRO Packet Insight	True	A
NE - FAS	StrataSync, Insights	Mitigated	-
NE – WBU	TM500	True	A
NE – WBU	TeraVM Classic, RDA, AI RSG TeraVM OST	True	A, B B
NE – FAS	Video VSA Monitor	True	B
NE – FAS	ONMSi	True	B

NE – FAS	XPERTrak	True	B
NE-L&P	FoPLT-MAP	False	-
NE-FAS	FIT-INX	False	-
NE-L&P	ONE LabPro & ONT	False	-
NE-FAS	Fiber FODAS (FTH-DAS)	True	B
NE-FAS	Fiber AMS	True	B
NE A&D	WFI Products (ONA-800, JD720x)	False	-
NE A&D	IL Products: All Products	False	-
NE A&D	PNT Products	False	-
NE A&D	All AvComm Products, (45TS, AVX10k, CX200, CX300, CX700)	False	-
NE A&D	TRX	False	-

NOTE: If your product is not listed, please reach out to Viavi support.

Recommended Short-Term Mitigation

Debian-Based Systems: Kernel Module Disable (Ubuntu, Amazon Linux, SUSE)

1. Disable the algif_aead module (Linux)

   Blacklist the module to prevent it from loading on next boot, then unload it from the running kernel:

   ```
   echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif-aead.conf
   rmmod algif_aead 2>/dev/null
   ```

2. Verify the module is no longer loaded:

   ```
   lsmod | grep algif_aead
   ```

A blank result confirms the module is unloaded.

RHEL-Based Systems: Kernel Module Blacklisting (RHEL, Oracle, Rocky)

1. Disable the algif_aead_int function by adding it to blacklist

   grubby --update-kernel=ALL --args="initcall_blacklist=algif_aead_init"

2. Reboot the system

   systemctl reboot

Recommended Medium-Term Mitigation

OS vendors are working through releasing software patches to deliver permanent patches to impacted module. One available for designated distro, recommendation is to proceed with the standard kernel update.

References

https://cert.europa.eu/publications/security-advisories/2026-005/

https://security.utoronto.ca/advisories/copy-fail-linux-kernel-lpe-and-container-escape/#:~:text=The%20vulnerability%20has%20been%20present,level%20mitigation%20are%20strongly%20recommended.

access.redhat.com/security/cve/cve-2026-31431