

CVE-2026-98564

Microsoft net: dsa: mt7530: leave the MDIO IRQ mappings to regmap-irq

In the Linux kernel, the following vulnerability has been resolved: net: dsa: mt7530: leave the MDIO IRQ mappings to regmap-irq mt7530_remove_common() disposes the per-PHY interrupt mappings from .remove, but the regmap-irq chip that owns the domain is devm-registered, so its parent interrupt is only freed once .remove has returned. The switch's own regmap-irq thread can therefore still dispatch on a mapping that is already gone: irq_find_mapping() returns 0, irq_to_desc() returns NULL and handle_nested_irq() locks

EVRS	CVSS	EPSS	CISA DEADLINE
0/100	—	0.002	—
Informational priority	Not scored	9th percentile · FIRST	No CISA deadline

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

☐ CISA KEV	Not currently CISA KEV-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEV listing date unavailable
☐ EPSS	0.002 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☐ CVSS	CVSS base score unavailable	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Monitor Untagged reference available; patch status is not confirmed

NVD lists one or more references for this CVE that aren't tagged as a patch or vendor advisory. Review them directly to confirm patch availability and applicability before making a remediation decision.

Basis: NVD reference (untagged)

desc->lock without checking it. The attached PHYs have not given those interrupts back yet either, which the kernel warns about a moment before the fault. regmap_del_irq_chip() disposes the same mappings itself, after freeing the parent interrupt and before removing the domain, so there is nothing left for the driver to do here. Until it runs the descriptors stay alive, and a late dispatch on one of them is harmless: dsa_unregister_switch() has freed the PHY handlers by then, so handle_nested_irq() finds no action and returns.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Not identified by the connected sources	—	no fixed version listed	NVD

Sources

Reference	git.kernel.org/stable/c/0d80ba0a204c6a16bd7778b50de578dff107c0fe	Additional reference	git.kernel.org/stable/c/2357c682f6eaf639dec88c68b3c0c93a3b802635
Additional reference	git.kernel.org/stable/c/f306e465b5a2091cd3fe3dd0feb10cfc94cfb2f8	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98564
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103609	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98564

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.