

CVE-2026-98480

Microsoft nfc: trf7970a: power down on startup RX gain failure

In the Linux kernel, the following vulnerability has been resolved: nfc: trf7970a: power down on startup RX gain failure
trf7970a_startup() powers up the device before applying the optional RX gain reduction. If the register read or write fails, it returns without undoing that power-up. Probe's unwind only drops the separate regulator references acquired by probe, leaving the additional VIN enable from startup unbalanced. The system resume caller also has no power-down on this error.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9th percentile · FIRST	CISA DEADLINE — 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)

Call trf7970a_power_down() before returning the RX gain error to deassert the enable GPIOs, release the startup VIN reference and restore the powered-off state. Runtime PM has not been enabled yet, so the full shutdown helper is not appropriate here. Preserve the original SPI error. This issue was identified during our ongoing static-analysis research while reviewing kernel code.

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/6ef70d790425e76b42c69e416ee78c62bdc37d00	Additional reference	git.kernel.org/stable/c/cc444e4ad43461374dd128573eccb8979d2adb4c
Additional reference	git.kernel.org/stable/c/d2acbde7e67df44efa8f0963462d1192e7694ffc	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98480
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103720	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98480

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