

CVE-2026-98781

Microsoft drm/mediatek: Fix pdev reference leak in mtk_drm_bind()

In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Fix pdev reference leak in mtk_drm_bind()
When the device is not the mmsys master, mtk_drm_bind() returns early after taking a reference on the disp-mutex device via of_find_device_by_node(), without ever dropping it: mtk_drm_unbind() only puts mutex_dev for the master. Drop the reference before returning from the non-master path.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.7th 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)

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/3753e34b73fcb2a2edbe984614a008a261697ef	Additional reference	git.kernel.org/stable/c/4a0ae61067671f556eeaf5ea4e59a1db63163d70
Additional reference	git.kernel.org/stable/c/4a8f9cad0fced77b36b297c67c42730c9cb32ec6	Additional reference	git.kernel.org/stable/c/b84f1386d84b3a73f73ebb416a3f97c5d64a8ab3
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98781	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103866
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98781		

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