

CVE-2026-98782

Microsoft drm/mediatek: Fix ovl adaptor platform device leak

In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Fix ovl adaptor platform device leak
mtk_drm_probe() creates an OVL adaptor platform device with platform_device_register_data() when the display pipeline requires the OVL adaptor. If a later initialization step fails, the probe error path releases the DRM resources without unregistering the already registered OVL adaptor device. The normal remove path likewise leaves the device registered after the DRM driver is unbound.

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

Keep track of whether the OVL adaptor was successfully registered and unregister it on probe failure. Also recover the platform device from the stored DDP component device and unregister it during normal removal. The issue was identified by a static analysis tool I developed and confirmed by manual review.

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/048739be3e9caca5301b68245668002fe6f0ce5	Additional reference	git.kernel.org/stable/c/3d85bd738aba61df14daf8fe638e2172d8427bf
Additional reference	git.kernel.org/stable/c/629458b7e49559593823e351535294db17331be7	Additional reference	git.kernel.org/stable/c/8e3a350075b556f2fed4517705935bfee4529fb6
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98782	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103867
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98782		

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