

CVE-2026-98783

Microsoft drm/mediatek: Add missing IS_ERR check for ovl_adaptor platform device

In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Add missing IS_ERR check for ovl_adaptor platform device platform_device_register_data() can fail and return an ERR_PTR, but the return value is used without checking, leading to an invalid pointer being stored in ddp_comp[].dev and passed to component_match_add() and mtk_ddp_comp_init(), which could result in a kernel crash. Add an IS_ERR() check to jump to the error handling path on failure.

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/4acac370aad2d4895a82f40b2f03e9ef70eeca6	Additional reference	git.kernel.org/stable/c/88f8a92dcb0cb154774595dee7226458de4cbd38
Additional reference	git.kernel.org/stable/c/aeef8a8537bcfb26689edb36ed905b8b2873001c	Additional reference	git.kernel.org/stable/c/bce7698e2e6565bb765bd0522337f29f5f312624
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98783	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103868
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98783		

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