

CVE-2026-98512

Microsoft drm/nouveau: RCU-free the scheduler-containing nouveau_sched

In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: RCU-free the scheduler-containing nouveau_sched struct nouveau_sched embeds a struct drm_gpu_scheduler (base). nouveau_sched_destroy() calls nouveau_sched_fini() (which does drm_sched_fini(&sched->base)) and then frees the object with plain kfree(sched). drm_sched_fence_get_timeline_name() returns fence->sched->name, and the scheduler fence keeps a .release callback so it is not ops-detached on signalling.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9.3rd 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)

A finished fence exported to userspace via drm_syncobj / sync_file therefore keeps pointing at &sched->base after nouveau_sched_destroy(), and a later get_timeline_name() -- reachable unprivileged through SYNC_IOC_FILE_INFO -- dereferences freed memory (KASAN slab-use-after-free read). Per the dma-fence lifetime contract the exporter must keep the data backing a signalled fence alive for an RCU grace period. Free the scheduler-containing object with kfree_rcu() instead of kfree().

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/35151e9a8274174ccbb92e3b3ba7dc7a008dcada	Additional reference	git.kernel.org/stable/c/40edf5eefc3fd94592a91d6eb074d4fc6f606c75
Additional reference	git.kernel.org/stable/c/cd6e11b6ebe04a0a1f1435df561acada9eadc563	Additional reference	git.kernel.org/stable/c/f7eae6d8d768fabd6b59779ca7da79e02c74e113
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98512	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103752
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98512		

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