

CVE-2026-98522

Microsoft drm/imagination: Propagate map failures correctly from pvr_mmu_map_sgl()

In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Propagate map failures correctly from pvr_mmu_map_sgl() Map failure from pvr_mmu_map_sgl() interface was not returned correctly to pvr_mmu_map() interface. This resulted in pvr_mmu_map() interface to continue instead of returning an error to caller. Fix it by returning a proper error code from pvr_mmu_map_sgl() interface.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 10.4th 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 stack for crash: [1179.286237] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 [1179.295067] Mem abort info: [1179.297877] ESR = 0x0000000096000004 [1179.301656] EC = 0x25: DABT (current EL), IL = 32 bits [1179.306987] SET = 0, FnV = 0 [1179.310048] EA = 0, S1PTW = 0 [1179.313198] FSC = 0x04: level 0 translation fault [1179.318096] Data abort info: [1179.320993] ISV = 0, ISS = 0x000000004, ISS2 = 0x00000000 [1179.326483] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [1179.331546] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [1179.336895] user pgtable: 4k pages, 48-bit VAs, pgdp=000000009822a000 [1179.343402] [0000000000000008] pgd=0000000000000000, p4d=0000000000000000 [1179.350243] Internal error: Oops: 0000000096000004 [#2] SMP [1179.355908] Modules linked in: powervr gpu_sched drm_shmem_helper drm_gpuvm drm_exec xhci_plat_hcd xhci_hcd dwc3 usbcore usb_common snd_soc_simple_card snd_soc_simple_card_utils dwc3_am62 at24 sa2ul sha512 libsha512 sha256 authenc sch_fq_codel fuse dm_mod ipv6 [1179.378992] CPU: 1 UID: 1000 PID: 680 Comm: deqp-vk Tainted: G D 6.17.0 #1 PREEMPT [1179.388120] Tainted: [D]=DIE [1179.390994] Hardware name: Texas Instruments AM625 SK (DT) [1179.396467] pstate: 00000005 (nzcw daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [1179.403415] pc : pvr_mmu_op_context_unmap_curr_page+0x6c/0x134 [powervr] [1179.410140] lr : pvr_mmu_op_context_unmap_curr_page+0x58/0x134 [powervr] [1179.416848] sp : ffff8000839ab8c0 [1179.420153] x29: ffff8000839ab8c0 x28: 0000000000000001 x27: 000000008f386000 [1179.427283] x26: ffff000016d1df98 x25: 0000000000247000 x24: 00000000000001e6 [1179.434413] x23: 0000000000000002 x22: 000000000000ffff x21: 0000000000000247 [1179.441540] x20: 0000000000000245 x19: ffff000016d1df60 x18: 0000000000000002 [1179.448668] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000001 [1179.455793] x14: 0000000000060810 x13: ffff80007ffffff x12: ffff00004190480 [1179.462921] x11: ffff8000853f7000 x10: ffff8000811ae000 x9: ffff000041900b8 [1179.470051] x8: 0000000000000000 x7: 00000000990c4001 x6: 0000000000000007 [1179.477177] x5: ffff000016d1df60 x4: 0000000000000000 x3: ffff00000a7d8000 [1179.484306] x2: 00000000000001ff x1: 0000000000000000 x0: 0000000000000000



[1179.491433] Call trace: [1179.493872] pvr_mmu_op_context_unmap_curr_page+0x6c/0x134 [powervr] (P)
[1179.500582] pvr_mmu_map+0x31c/0x388 [powervr] [1179.505027] pvr_vm_gpuva_map+0x40/0x88 [powervr]
[1179.509732] __drm_gpuvm_sm_map+0x250/0x44c [drm_gpuvm] [1179.514952] drm_gpuvm_sm_map+0x48/0x5c
[drm_gpuvm] [1179.519822] pvr_vm_bind_op_exec+0x64/0x70 [powervr] [1179.524785] pvr_vm_map+0x1f8/0x2a8
[powervr] [1179.529142] pvr_ioctl_vm_map+0x12c/0x188 [powervr] [1179.534018] drm_ioctl_kernel+0xb8/0x128
[1179.537941] drm_ioctl+0x21c/0x4ec [1179.541337] __arm64_sys_ioctl+0xac/0x108 [1179.545344]
invoke_syscall+0x44/0x100 [1179.549091] el0_svc_common.constprop.0+0x40/0xe0 [1179.553790] do_el0_svc+0x1c/0x28
[1179.557106] el0_svc+0x34/0xf0 [1179.560159] el0t_64_sync_handler+0xd0/0xe4 [1179.564334]
el0t_64_sync+0x198/0x19c [1179.567996] Code: 54000300 35000360 f9402261 79409a62 (f9400421) [1179.574081] ---
[end trace 0000000000000000]---

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/13c7ae1d92ceea18d55612fa9431ca5ac77025f5	Additional reference	git.kernel.org/stable/c/7b824c293a6b56de8285a97984c507cba56bc4c4
Additional reference	git.kernel.org/stable/c/afe5b4d66d45b278ecd0e3d6889fb208ce2e5339	Additional reference	git.kernel.org/stable/c/d30ea2747164992f5e720f6f53695d422bdc0346
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98522	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103762
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98522		

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