

CVE-2026-98523

Microsoft drm/client: fix restore of partially initialized client

In the Linux kernel, the following vulnerability has been resolved: drm/client: fix restore of partially initialized client I got a null-
ptr-deref report when closing a DRM file descriptor: WARNING: drivers/gpu/drm/drm_atomic.c:2031 at
__drm_atomic_helper_set_config+0x18e/0x1b0 [drm] Call Trace: drm_client_modeset_commit_atomic+0x16b/0x220 [drm]
drm_client_modeset_commit_locked+0x56/0x160 [drm] drm_client_modeset_commit+0x21/0x40 [drm]
__drm_fb_helper_restore_fbdev_mode_unlocked.part.0+0x7b/0x80

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)

drm_fbdev_client_restore+0xe/0x20 [drm_client_lib] drm_client_dev_restore+0x9f/0xc0 [drm] drm_release+0xc5/0xe0 [drm]
The warning is followed by a NULL pointer dereference: BUG: kernel NULL pointer dereference, address: 0000000000000008
RIP: __drm_fb_helper_restore_fbdev_mode_unlocked.part.0+0x41/0x80 [drm_kms_helper] Call Trace:
drm_fbdev_client_restore+0xe/0x20 [drm_client_lib] drm_client_dev_restore+0x9f/0xc0 [drm] drm_release+0xc5/0xe0 [drm]
__fput+0xdc/0x2b0 __x64_sys_close+0x39/0x80 do_syscall_64+0x8d/0x460 entry_SYSCALL_64_after_hwframe+0x76/0x7e
drm_client_register() adds the DRM client to the device client list before invoking the initial hotplug callback. If the hotplug
callback fails, the client remains registered. For the fbdev client, a failure during drm_fb_helper_initial_config() causes the
partially initialized fbdev helper to be cleaned up. drm_fb_helper_fini() releases fb_helper->info and leaves it NULL. The fbdev
client therefore remains registered even though there is no fully initialized framebuffer device. Later, when userspace closes
the DRM file descriptor, drm_release() can invoke the restore callbacks of registered DRM clients: drm_release()
drm_client_dev_restore() drm_fbdev_client_restore() drm_fb_helper_restore_fbdev_mode_unlocked() drm_fbdev_client_restore()
currently restores the fbdev state unconditionally. For a partially initialized fbdev client this can submit an incomplete modeset
state and subsequently access fbdev state which has not been initialized, resulting in the warning and NULL pointer
dereference above. drm_fbdev_client_unregister() already uses fb_helper->info to distinguish a fully probed framebuffer device
from a partially initialized client. Use the same condition in drm_fbdev_client_restore() and skip restore if no framebuffer device
has been successfully initialized.

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/11edd5b6735d2e1069ddce672b1836713647f7fb	Additional reference	git.kernel.org/stable/c/1fca688e9443003e33cf30453e7a7560367656c9
Additional reference	git.kernel.org/stable/c/a69c4b678db808c0d89abb8cedaaaac38d1ef182	Additional reference	git.kernel.org/stable/c/fcbdba553a9c430079ee225df2dc7ab556a2f83
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98523	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103763
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98523		

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