

CVE-2026-98313

Microsoft drm/msm/dp: skip PUSH_IDLE when the link was never enabled

In the Linux kernel, the following vulnerability has been resolved: drm/msm/dp: skip PUSH_IDLE when the link was never enabled. `msm_dp_display_atomic_enable()` returns early when link training fails, leaving `->power_on` false and the main link down. `msm_dp_display_atomic_disable()` nevertheless writes `DP_STATE_CTRL_PUSH_IDLE` and waits for an idle-pattern completion that cannot arrive, so every failed enable is followed by "PUSH_IDLE pattern timeout".

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 6.4th 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)

Every other step of the teardown is already gated on that flag: `msm_dp_display_disable()`, called from `.atomic_post_disable()`, returns early on `!power_on`. The `PUSH_IDLE` write is the only one that is not, so the controller's runtime-PM reference is then dropped without the link having been taken down. On glymur (Snapdragon X2 Elite) the consequence is not a warning. The SoC does not survive it: TrustZone force-stops the SOCCP and ADSP remote processors and the machine resets silently about 50 ms later, with no oops and no panic. On an ASUS Zenbook A16 (UX3607OA), whose eDP panel does not currently train, this reproduces without any compositor or GPU involvement: # eDP enable has already failed with "Failed link training (rc=-104)"
`echo 1 > /sys/class/graphics/fb0/blank [535.645455] === marker === [535.694833] qcom_q6v5_pas d00000 remoteproc: fatal error received: \ sys_m_smsm.c:512:TZ force stop [535.694875] remoteproc remoteproc0: crash detected in soccp: type fatal error [535.728857] qcom_q6v5_pas 6800000 remoteproc: fatal error received: \ sys_m_smsm.c:783:err fatal notification received from TZ <SoC reset> Gate the PUSH_IDLE write on ->power_on so the disable path is consistent with the rest of the teardown. With this applied the same sequence is harmless and the machine stays up; without it, it resets every time. The unconditional write dates back to the original DP driver (c943b4948b58 ("drm/msm/dp: add displayPort driver support")), but the surrounding code has been restructured several times since, so no Fixes: tag is offered. Note that the eDP link-training failure that exposes this on the A16 is a separate problem in the glymur eDP PHY and is reported separately; this change is about not damaging the machine when training fails, for whatever reason. Tested on ASUS Zenbook A16 (UX3607OA), Snapdragon X2 Elite Extreme, on linux-next next-20260803 and next-20260807. The machine has since been running next-20260807 with this patch as its daily driver. Patchwork: https://patchwork.freedesktop.org/patch/745167/`



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/5e97d117b79c3ce89542369ef697be64850de8ad	Additional reference	git.kernel.org/stable/c/dc57147549a10c99766144cde265645287718ff7
Additional reference	git.kernel.org/stable/c/e249a6e2a130c08bb4d8b0a55cbe29754307e5c9	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98313
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93298	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98313

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