

CVE-2026-98841

Microsoft virt: vmgenid: set driver_data before registering notification handlers

In the Linux kernel, the following vulnerability has been resolved: virt: vmgenid: set driver_data before registering notification handlers Both probe paths register their notification handler before assigning driver_data, which the handler dereferences. In the devicetree path, the notification IRQ can fire as soon as devm_request_irq() registers the handler: the interrupt may already be pending at probe time, for example when a VMM injects the generation-changed notification while restoring a guest from a snapshot

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)

that was taken before the driver had probed (Firecracker does exactly this on snapshot restore). The IRQ is also requested with IRQF_SHARED, so another device sharing the line can trigger the handler just as early. The handler then calls vmgenid_notify(), which dereferences the still-NULL driver_data and panics: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000010 CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.18.38+ #1 PREEMPT(none) Hardware name: linux,dummy-virt (DT) pc : vmgenid_notify.isra.0+0x24/0x8c Ir : vmgenid_of_irq_handler+0x14/0x34 Call trace: vmgenid_notify.isra.0+0x24/0x8c (P) vmgenid_of_irq_handler+0x14/0x34 __handle_irq_event_percpu+0x44/0x1bc handle_irq_event+0x4c/0xb4 handle_fasteoi_irq+0xf8/0x1f8 The ACPI path has the same ordering problem: the handler is installed with acpi_install_notify_handler() before driver_data is assigned. ACPI notifications are dispatched asynchronously from a workqueue, so the window is narrow, but a notification arriving between the two calls hits the same NULL dereference. Assign driver_data before registering the handlers. The state is fully initialized at that point, so the handlers are safe to run. Should registration fail, the probe error path leaves no dangling pointer behind: the driver core clears driver_data in device_unbind_cleanup().



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/538fe5efaa9704ad820ba34b4f9df135ca873d79	Additional reference	git.kernel.org/stable/c/7a1e8daaaa466c6aaffa223e1afe9cfeece0dd47
Additional reference	git.kernel.org/stable/c/8f42954ad8bf9bdbf574f2c437ad30cb2601f401	Additional reference	git.kernel.org/stable/c/9f8139c6145cf17d690d6c414d43b4c0bef632fb
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98841	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103781
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98841		

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