

CVE-2026-98804

Microsoft net: page_pool: fix use-after-free in page_pool_recycle_ring_bulk()

In the Linux kernel, the following vulnerability has been resolved: net: page_pool: fix use-after-free in page_pool_recycle_ring_bulk() With CONFIG_PAGE_POOL_STATS=y, page_pool_recycle_ring_bulk() updates the recycle stats after dropping the producer lock. If it just recycled the last inflight netmems of a pool being destroyed, page_pool_release() can pass its producer-lock barrier and free the pool before recycle_stat_add() runs.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9th 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)

Commit fcc680a647ba7 ("page_pool: allow mixing PPs within one bulk") moved this stat update after the unlock. Commit 271683bb2cf32 ("page_pool: Fix use-after-free in page_pool_recycle_in_ring") later added the barrier, but only fixed page_pool_recycle_in_ring(). Move the update back under the lock.

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/0b105f4eb78e5ee39e5a74c47c9efd69b6ac849c	Additional reference	git.kernel.org/stable/c/bdea4980182e3badac74f04df6c07492b91c569e
Additional reference	git.kernel.org/stable/c/f78d45d5f1ac4141a03f033141368671da4293e4	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98804
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103889	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98804

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