

CVE-2026-98858

Microsoft io_uring: fix task_work add use-after-free with SQPOLL

In the Linux kernel, the following vulnerability has been resolved: io_uring: fix task_work add use-after-free with SQPOLL For SQPOLL, the sqpoll thread runs task_work off its own list and doesn't need to be told about it, so it can pop and complete a request as soon as mpسق_push() has published it. If that was the last request holding the ring alive, io_ring_exit_work() then frees the ctx, stops the thread, and with it the tctx, while io_req_normal_work_add() is still looking at both after the push: BUG: KASAN:

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 4.4th percentile · FIRST	CISA DEADLINE — No CISA deadline
---	---------------------------------------	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

☐ CISA KEY	Not currently CISA KEY-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 KEY 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)

slab-use-after-free in io_req_normal_work_add+0x439/0x510 Read of size 4 at addr ff11000000ca0000 by task repro/55 (...) BUG: KASAN: slab-use-after-free in queue_work_on+0x25/0x70 Write of size 8 at addr ff11000000c3bd00 by task repro/55 Hold an RCU read lock across the add, like io_req_local_work_add() already does, and have io_ring_exit_work() wait for a grace period for SQPOLL rings as well before freeing the ctx.

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/395b25968fe854d4efaa19a8e9b7a5b6d1b3eea3	Additional reference	git.kernel.org/stable/c/42b3332efacfd2140be4cd0dedad4fb96b8ae90e
Additional reference	git.kernel.org/stable/c/891bd8335a0de3bb15c3b797ce3026bbb0dbef6c	Additional reference	git.kernel.org/stable/c/a92193c91e8839fe5fc209616ea95465ae4b919d
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98858	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103798
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98858		

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