

CVE-2026-98821

Microsoft block: reject polled dio with user integrity metadata

In the Linux kernel, the following vulnerability has been resolved: block: reject polled dio with user integrity metadata IOCB_HAS_METADATA leaves iocb->private as a uio_meta, while iocb_bio_iopoll() expects a bio. Since 2729a60bbfb9, metadata I/O always uses __blkdev_direct_IO(), which never publishes the bio for polling, so IOPOLL calls bio_poll() on the uio_meta. Reproducer: io_uring IOPOLL plus a PI attribute on an integrity device (scsi_debug dif=1 dix=1).

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.5th 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)

KASAN reports: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000004 KASAN: null-ptr-deref in range [0x0000000000000020-0x0000000000000027] RIP: 0010:bio_poll+0x9d/0x4b0 Call Trace: iocb_bio_iopoll+0x5b/0x80 io_uring_classic_poll+0xf3/0x140 io_do_iopoll+0x4e3/0xc00 io_iopoll_check+0x275/0x560 __do_sys_io_uring_enter+0x2e5/0x720 Return -EOPNOTSUPP when HIPRI is combined with user metadata.

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/2a42e6fe1293f2e2d579c9fe5bbab056dd8b880e	Additional reference	git.kernel.org/stable/c/c97ef13ad96be0e08af38dfa2ed40cded0b53e1b
Additional reference	git.kernel.org/stable/c/dd33c03cefccdfcb223e9e6262643d64f8c1ae20	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98821
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103906	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98821

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