

CVE-2026-98680

Microsoft iio: accel: kionix-kx022a: Prevent memory leak and fix state

In the Linux kernel, the following vulnerability has been resolved: iio: accel: kionix-kx022a: Prevent memory leak and fix state
The driver allocates memory for samples at buffer enable path. If regmap operation fails in the kx022a_fifo_enable() at the buffer enable path, the allocated memory is never freed. Furthermore, the state information and previous hardware configuration(s) aren't undone, potentially leaving WMI interrupts and buffers enabled, or driver state flags wrong. Free the memory and revert the hardware configuration and state flags on error path.

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)

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/2ef953f7b54e1460718116b4c0a4c63b106348fc	Additional reference	git.kernel.org/stable/c/5c7ca8fe72064c1c3c7a7418031f692bb2bffa260
Additional reference	git.kernel.org/stable/c/e3bc345d08639e62b629e0ec0799f7fb45e21372	Additional reference	git.kernel.org/stable/c/e65e128b51a37dd1a9056ac3d1705d805a5c8bb0
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98680	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103934
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98680		

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