

CVE-2026-98676

Microsoft iio: adc: ade9000: fix NULL pointer dereference in clkout registration

In the Linux kernel, the following vulnerability has been resolved: iio: adc: ade9000: fix NULL pointer dereference in clkout registration ade9000_setup_clkout() passes NULL as the register address when registering a divider clock. During clock registration, the common clock framework calls clk_divider_recalc_rate(), which dereferences the address through readl(). As a result, probing an ADE9000 configured as a clock provider with an external input clock crashes.

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)

CLKOUT passes CLKIN through without changing its rate. Register it as a 1:1 fixed-factor clock, which does not require register access. This change does not affect the configuration using the internal clock, for which the driver does not register a clock provider.

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/134aa31a8d4e71f6ab1d155ad7b4502508832f72	Additional reference	git.kernel.org/stable/c/49ee1c6a3ebda6b7de06b2961b0e09c1c3fe536a
Additional reference	git.kernel.org/stable/c/d2400175228fbc10b29c49a7b5f70a7e80d144dd	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98676
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103930	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98676

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