

CVE-2026-98528

Microsoft gpio: cdev: fix kernel stack leak to user-space in error path

In the Linux kernel, the following vulnerability has been resolved: gpio: cdev: fix kernel stack leak to user-space in error path If we fail to acquire the GPIO chip guard in gpio_desc_to_lineinfo(), we return immediately before zeroing the info struct we'll end up passing to the user-space later in lineinfo_get_v1(). This may leak the kernel stack contents. Make gpio_desc_to_lineinfo() return int so that the -ENODEV returned on failure to acquire the guard can be propagated to the callers.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 10.4th 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)

While not strictly necessary: move the memset() before trying to acquire the SRCU read lock too for good measure.

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/1feb5d39b05afd902ed9fc902ec5b15be03a4bdb	Additional reference	git.kernel.org/stable/c/60a466f231905cd96ae6f0f3c44a710c97873dac
Additional reference	git.kernel.org/stable/c/8460ee5216ab9a38263b01dca4b0a27e083f70f3	Additional reference	git.kernel.org/stable/c/cf3d043582e106a0e57002bec8a6de8929ba3e1c
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98528	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103573
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98528		

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