

CVE-2026-98235

Microsoft net/sched: act_api: release tail references on DELACTION failure

In the Linux kernel, the following vulnerability has been resolved: net/sched: act_api: release tail references on DELACTION failure A batched RTM_DELACTION request takes a temporary reference on each action before attempting any deletion. tcf_action_delete() clears each processed slot and drops its temporary reference before attempting the deletion.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 6.6th 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)

If deletion fails, tca_action_gd() calls tcf_action_put_many() to release the remaining references, but its tcf_act_for_each_action() iterator stops at the first NULL slot. When a batch stops at an action bound to a filter, this leaks a reference on each subsequent action. A later delete of an unbound action can then return success without removing it from the IDR. Walk the full array in tcf_action_put_many() and skip NULL slots to release the references held on the unprocessed actions.

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/1be63e4579af408d596f0f3165faf1a880631d3b	Additional reference	git.kernel.org/stable/c/57b477e46ef2df3483f3488cc713c61c4b384aab
Additional reference	git.kernel.org/stable/c/6e05e46fa821a5c1b281355f1f622ac76cb6080a	Additional reference	git.kernel.org/stable/c/9eaba16f1b6ee19b249e6afd82c27f958d441458
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98235	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93163
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98235		

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