

CVE-2026-98534

Microsoft ipe: fix use-after-free when auditing a newly loaded policy

In the Linux kernel, the following vulnerability has been resolved: ipe: fix use-after-free when auditing a newly loaded policy
new_policy() audits the policy after ipe_new_policyfs_node() publishes it and drops the new directory's inode lock. A concurrent delete can free the policy while ipe_audit_policy_load() is still using it. Audit the successful load under that lock. [FW: remove model name according to latest guideline]

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 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/48f7d0233c3cc8d986d1177d0e5dd4af435e7265	Additional reference	git.kernel.org/stable/c/9814077275eca36ebf8d510d2f076d235ff9f51a
Additional reference	git.kernel.org/stable/c/b72d6c72b4bfb021e8e127fa13e0f27d09be737	Additional reference	git.kernel.org/stable/c/e9015d32752fa228ef2f0e07fd93fc53a4a4c723
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98534	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103579
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98534		

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