

CVE-2026-98543

Microsoft bpf: fs/xattr: don't assume the inode is locked in path_unlink/path_rmdir

In the Linux kernel, the following vulnerability has been resolved: bpf: fs/xattr: don't assume the inode is locked in path_unlink/path_rmdir bpf_lsm_has_d_inode_locked() makes the verifier rewrite bpf_[set|remove]_dentry_xattr() to the _locked variants, which assume that the caller already holds the inode's i_rwsem. The path_unlink and path_rmdir hooks are listed, but security_path_unlink() and security_path_rmdir() run before vfs_unlink()/vfs_rmdir() take the victim inode's i_rwsem, so a sleepable BPF LSM program

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)

attached to either hook mutates the victim's xattrs without the lock held. Drop the two path hooks from d_inode_locked_hooks so that the verifier keeps the locking bpf_[set|remove]_dentry_xattr() variants, which take the lock themselves.

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/35d442ed1f86465e49df3119fb898f985186db13	Additional reference	git.kernel.org/stable/c/640d37fbd34d03af727dbc567f48c0203d1de6b4
Additional reference	git.kernel.org/stable/c/7504b677c4370c9e4b153c553ff8831c093b1ff6	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98543
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103588	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98543

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