

CVE-2026-98420

Microsoft ksmbd: follow SMB2 session expiration semantics

In the Linux kernel, the following vulnerability has been resolved: ksmbd: follow SMB2 session expiration semantics
ksmbd_session_register() destroys valid sessions after ten seconds of inactivity whenever a client starts another SessionSetup exchange. This confuses Session.IdleTime with Session.ExpirationTime. Windows can create additional authenticated sessions on an existing connection, so deleting the older session invalidates its tree connects and makes mapped drives fail with STATUS_NETWORK_NAME_DELETED.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 13.8th 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)

The session expiration rules require the server to change a valid session to expired only after its credential expiration time passes. A valid or expired session otherwise keeps its connection from being scavenged. Connections that have not negotiated a dialect, have no sessions, or have only InProgress sessions are disconnected after an implementation-specific timeout. Use the Windows-compatible 45 second value and run the expiration check periodically for both TCP and SMB Direct. Keep zero as an infinite credential expiration time, and count each Valid-to-Expired transition. Set expired sessions to InProgress when they reauthenticate. If authentication fails, remove the session from the global and per-connection tables immediately, including SMB3 multichannel connections. Retain protection against abandoned SessionId-zero exchanges by allowing only one InProgress authentication per connection. Additional exchanges fail with STATUS_INSUFFICIENT_RESOURCES, and stale InProgress sessions are reaped after the same 45 second setup timeout. This bounds the original unauthenticated memory-exhaustion path without evicting established sessions.

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/c99ea7855124ca1428a1e59c2b4590aaef34eacf

NVD nvd.nist.gov/vuln/detail/CVE-2026-98420

Current data evulnable.com/vulnerability-management/cve/CVE-2026-98420

Additional reference git.kernel.org/stable/c/d7fd1f98607f2cd358e583f9548bdf0173090a86

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-101069

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