

CVE-2026-98274

Microsoft net: psp: avoid conflicts with skb->decrypted and sk_validate_xmit_skb()

In the Linux kernel, the following vulnerability has been resolved: net: psp: avoid conflicts with skb->decrypted and sk_validate_xmit_skb() PSP conflicts with TLS ULP in its usage of both skb->decrypted and sk->sk_validate_xmit_skb(). Make PSP mutually exclusive with TLS ULP, the only other user of either of these. As other users of skb->decrypted come along, they can be added to sk_has_decrypt_user().

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 6.4th 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)

It would make sense to also assert that sk->sk_validate_xmit_skb() is also NULL in both of these setup paths for similar future proofing, but the PSP listener/sk_clone() path is still broken and it could be seen as a regression to not allow rx assoc to run on a child of a listener socket with PSP tx assoc state. Include all TCP ULPs in the sk_has_decrypt_user() check, even though TLS is the only one that conflicts with PSP via the decrypted bit. This is intentional because PSP was not designed to be used with ULPs. It is best to close off surface area that may make bugs reachable, until someone wishes to design and test an actual user of PSP with ULPs.

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/a13cca5ba5375f13cbdab545abfb5e288bef3f78	Additional reference	git.kernel.org/stable/c/a41f24c612c3f5139a3143307eb85bbcf1bd4d07
Additional reference	git.kernel.org/stable/c/c8c8c18862337c469e325c207601de3279847809	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98274
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93202	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98274

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