

CVE-2026-98230

Microsoft xfrm: use hlist_del_init_rcu for state_cache and state_cache_input

In the Linux kernel, the following vulnerability has been resolved: xfrm: use hlist_del_init_rcu for state_cache and state_cache_input Commit 14acf9652e56 ("xfrm: defensively unhash xfrm_state lists in __xfrm_state_delete") converted bydst/bysrc/byseq/byspi from hlist_del_rcu() to hlist_del_init_rcu() so that a second __xfrm_state_delete() on the same object becomes a no-op rather than a write through LIST_POISON pprev.

EVRS 11 /100 Elevated priority	CVSS V3.1 7.0 High · NVD	EPSS 0.001 1.6th percentile · FIRST	CISA DEADLINE — No CISA deadline
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted evidence for 3 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	0.001 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Scheduled Maintenance Patch or fixed version identified
Basis: External remediation intelligence

It missed state_cache and state_cache_input, which kept hlist_del_rcu(): - hlist_del_rcu() leaves pprev = LIST_POISON2 (non-NULL), so hlist_unhashed() returns false. - hlist_del_init_rcu() leaves pprev = NULL, so hlist_unhashed() returns true. A second __xfrm_state_delete() therefore enters __hlist_del() on the already-deleted state_cache/state_cache_input nodes and does WRITE_ONCE(*pprev, next) through LIST_POISON2 — a write use-after-free once the slab is reused. The corruption can in turn cause a subsequent hlist_for_each_entry_rcu traversal to follow a dangling next pointer, producing the read use-after-free reported in xfrm_input_state_lookup(). Switch state_cache and state_cache_input to hlist_del_init_rcu() to match the other four lists, closing the write use-after-free and, with it, the read use-after-free it spawns.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Not identified by the connected sources	—	no fixed version listed	NVD

Sources

Vendor guidance	git.kernel.org/stable/c/2afb8dc1f4390f164db8352f8e685e126e9db566	Additional guidance	git.kernel.org/stable/c/4748c27e2e6a1969e02f1df46e62f79d2799b80b
Additional guidance	git.kernel.org/stable/c/9b74a47a4cbd0d29faff4f3b199212c73e6b6220	Additional guidance	git.kernel.org/stable/c/fb38fb7420d5f7192f9e2b6ac835ede149cd7ac5
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98230	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93158
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98230		

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