

CVE-2026-98258

Microsoft posix-cpu-timers: Prevent freeing a timer which is queued on the expiry list

In the Linux kernel, the following vulnerability has been resolved: posix-cpu-timers: Prevent freeing a timer which is queued on the expiry list Kijo analyzed another race in the POSIX CPU timer code: Commit bf635681c906 converted cpu_timer::firing from a tristate value to a boolean. This lost the distinction between "not owned by the firing list" and "still owned, but delivery was canceled".

EVRS 12 /100 Elevated priority	CVSS V3.1 7.8 High · NVD	EPSS 0.001 2.8th 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 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

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

The resulting race is: expiry handler timer_settime() timer_delete() ----- collect timer onto private firing list firing = true observes firing = true firing = false return TIMER_RETRY wait for handler observes firing = false finish deletion unhash and free timer resume list traversal read freed elist.next -> UAF The firing bit is clearly the wrong indicator since that commit. Check whether the timer is queued on the expiry list or not instead. If it is queued clear the firing bit to prevent signal delivery as before and return TIMER_RETRY so the caller unlocks the timer which allows the expiry code to make progress and remove it from the list.

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/4336e3f47d9d516441066e9a65eaf076790d8d45	Additional guidance	git.kernel.org/stable/c/9971dac1a77845ff467146915fcb9170f6a8209
Additional guidance	git.kernel.org/stable/c/c21eaa72f02fc6e85621cbe09d303d8fb8bd39cd	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98258
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93186	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98258

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