

CVE-2026-98552

Microsoft perf/core: Fix a refcount leak in attach_perf_ctx_data()

In the Linux kernel, the following vulnerability has been resolved: perf/core: Fix a refcount leak in attach_perf_ctx_data() The attach_perf_ctx_data() can race on global and !global cases. The global case is protected by global_ctx_data_rwlock and shares a single reference count using perf_ctx_data.global field. But when it races with !global case, it may miss to set the global field and result in a reference count leak.

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 KEY	Not currently CISA KEY-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 KEY 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)

```
CPU1 CPU2 ----- attach_task_ctx_data(global=1)
attach_task_ctx_data(global=0) cd1 = alloc_perf_ctx_data(); cd2 = alloc_perf_ctx_data(); // { .global = 0, .refcount = 1 };
try_cmpxchg(); // success, // task->perf_ctx_data = cd2 try_cmpxhg(); // fail; old = cd2 refcount_inc_not_zero(&old->refcount); //
success // old.refcount = 2 free_perf_ctx_data(cd1); Then later detach_global_ctx_data() will see the data but it's not marked as
global, so it won't call detach_task_ctx_data().
```

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/23250517cd475367653f1e99396967f54c6f1b7c	Additional reference	git.kernel.org/stable/c/5286d4eb5cd7e10d7d93c3cc596e18bc8ad80f72
Additional reference	git.kernel.org/stable/c/cca4980630b3c7a85f53cb43c6018184ce5d4e37	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98552
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103597	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98552

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