

CVE-2026-98542

Microsoft cgroup/cpuset: Return PERR_NOCPUS in remote_partition_enable() on subpartitions_cpus conflict

In the Linux kernel, the following vulnerability has been resolved: cgroup/cpuset: Return PERR_NOCPUS in remote_partition_enable() on subpartitions_cpus conflict When a remote partition is created underneath an existing local partition via a non-partition (PRS_MEMBER) intermediate cgroup, update_prstate() sees parent->partition_root_state == PRS_MEMBER and calls remote_partition_enable().

EVRS	CVSS	EPSS	CISA DEADLINE
0/100 Informational priority	— Not scored	0.002 9th percentile · FIRST	— 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)

Commit 86888c7bd117 ("cgroup/cpuset: Add warnings to catch inconsistency in exclusive CPUs") replaced the cpumask_intersects(tmp->new_cpus, subpartitions_cpus) error check in remote_partition_enable() with WARN_ON_ONCE(). As a result, remote_partition_enable() emits a warning and proceeds to enable the remote partition on CPUs that are already owned by the ancestor local partition in subpartitions_cpus. This can be reproduced on Linux 7.3.0-rc3 with: mkdir -p /tmp/cg1 mount -t cgroup2 none /tmp/cg1 echo "+cpuset" > /tmp/cg1/cgroup.subtree_control mkdir /tmp/cg1/A echo 1 > /tmp/cg1/A/cpuset.cpus echo 1 > /tmp/cg1/A/cpuset.cpus.exclusive echo root > /tmp/cg1/A/cpuset.cpus.partition echo "+cpuset" > /tmp/cg1/A/cgroup.subtree_control mkdir /tmp/cg1/A/B echo 1 > /tmp/cg1/A/B/cpuset.cpus echo 1 > /tmp/cg1/A/B/cpuset.cpus.exclusive echo "+cpuset" > /tmp/cg1/A/B/cgroup.subtree_control mkdir /tmp/cg1/A/B/D echo 1 > /tmp/cg1/A/B/D/cpuset.cpus echo 1 > /tmp/cg1/A/B/D/cpuset.cpus.exclusive echo root > /tmp/cg1/A/B/D/cpuset.cpus.partition which triggers: WARNING: kernel/cgroup/cpuset.c:1594 at remote_partition_enable+0x1c1/0x300 and leaves both /tmp/cg1/A and /tmp/cg1/A/B/D as active root partitions claiming exclusive CPU 1. Fix this by returning PERR_NOCPUS when tmp->new_cpus intersects subpartitions_cpus in remote_partition_enable(), matching the error code used by remote_cpus_update() for the same subpartitions_cpus conflict, and add a regression test case to tools/testing/selftests/cgroup/test_cpuset_prs.sh. Tested in QEMU on Linux 7.3.0-rc3 using the reproducer above and tools/testing/selftests/cgroup/test_cpuset_prs.sh.



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/0751ab665cb3dcdac224b002565f2e28461740d5	Additional reference	git.kernel.org/stable/c/241e67b60308cdce25bba66616a109759edd1d40
Additional reference	git.kernel.org/stable/c/31c88350b7dd1522792f726f79607f31bb55c50f	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98542
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103587	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98542

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