

CVE-2026-98788

Microsoft futex: Fix private hash use-after-free on resize

In the Linux kernel, the following vulnerability has been resolved: futex: Fix private hash use-after-free on resize
poll_state_synchronize_rcu(mm->futex.phash.batches) is used by futex_ref_drop() to check that a grace period has passed since the current hash was published. This relies on batches referencing a grace period which started after the hash pointer was assigned.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 4.3rd 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)

__futex_pivot_hash() sets mmph->batches before it replaces mmph->hash: scoped_guard(rcu) { mmph->batches = get_state_synchronize_rcu(); rcu_assign_pointer(mmph->hash, new); } The scoped_guard(rcu) doesn't stop new grace periods from starting, and if one starts between those two assignments, futex_ref_drop() can move forward while a reader still holds a pointer to the old hash. Fix things by setting mmph->batches after assigning mmph->hash. The scoped_guard(rcu) isn't needed, so let's drop that as well.

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/5d5dc18b3a9ac011619b7d3af4514bf9e9b6a6af
NVD nvd.nist.gov/vuln/detail/CVE-2026-98788

Additional reference git.kernel.org/stable/c/f35e3b5784221654f9cddb622275a7fa203f6c3
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-103873

Current data evulnable.com/vulnerability-management/cve/CVE-2026-98788

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