

CVE-2026-98281

Microsoft futex: Also allocate private hash on vfork()

In the Linux kernel, the following vulnerability has been resolved: futex: Also allocate private hash on vfork() As Jann demonstrated, it is entirely feasible to access the mm through vfork(). Therefore we need to allocate a private hash on vfork() as well as any other CLONE_VM user. Specifically, it must be avoided to have (private) futex waiters before allocating the private hash.

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

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/5468a4855b63b30156a79e5248e01bf1a2c18dd7	Additional guidance	git.kernel.org/stable/c/b61b6f95d6722dbbbd09e689fa41b55fd36f9a5
Additional guidance	git.kernel.org/stable/c/eecebafa8cabb4d1482f6a5e2acc25a8f934681b	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98281
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93209	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98281

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