

CVE-2026-98376

Microsoft bpf: Use array_map_meta_equal for percpu array inner map replacement

In the Linux kernel, the following vulnerability has been resolved: bpf: Use array_map_meta_equal for percpu array inner map replacement percpu_array_map_ops.map_meta_equal points to the generic bpf_map_meta_equal(), which does not compare max_entries. When a percpu array serves as an inner map, replacing it with one that has fewer max_entries bypasses the check.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.001 3.6th 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	0.001 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)

Since percpu_array_map_gen_lookup() inlines the original template's index_mask as a JIT immediate, a lookup on the replacement map can access pptrs[] out of bounds. Point percpu_array_map_ops.map_meta_equal to array_map_meta_equal(), which already enforces the max_entries equality check. Add a selftest to verify that replacing a percpu array inner map with a differently-sized one is rejected.

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/593980175389a05793f6060aa20e626330960395	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98376
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-95531	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98376

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