

CVE-2026-98611

Microsoft bpf: Check params size before reading reserved fields

In the Linux kernel, the following vulnerability has been resolved: bpf: Check params size before reading reserved fields
bpf_crypto_ctx_create() is a kfunc whose second argument is declared with the __sz annotation, so the verifier only guarantees that params__sz bytes of params are valid. The function nevertheless reads params->reserved[0] and params->reserved[1] (offsets 14 and 15) before comparing params__sz against the size of struct bpf_crypto_params, so a BPF program can pass a shorter buffer and have the

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.7th 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)

kernel read past the region that was validated for it. Move the size check in front of the reserved field reads.

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/86a0e945fb645ea90233fde239cd2de79f01974c	Additional reference	git.kernel.org/stable/c/a11212910cf09b2fe8db9afa41ef60c4f81879c5
Additional reference	git.kernel.org/stable/c/cd12d3e08620257fbcaa262785d7f4b9473afc7a	Additional reference	git.kernel.org/stable/c/e03253f5d65ebcd2a6d479f140c3bd9c7e4fb84a
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98611	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103656
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98611		

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