

CVE-2026-98196

Microsoft wifi: brcmsmac: fix UAF in brcms_free_timer()

In the Linux kernel, the following vulnerability has been resolved: wifi: brcmsmac: fix UAF in brcms_free_timer() brcms_free_timer() calls brcms_del_timer() which uses the non-synchronous cancel_delayed_work() to cancel the timer's underlying delayed work. If the work callback (_brcms_timer) is already running, cancel_delayed_work() returns false without waiting, and brcms_free_timer() proceeds to kfree(t) while the callback still accesses t through container_of().

EVRS	CVSS	EPSS	CISA DEADLINE
0/100 Informational priority	— Not scored	0.002 7.6th percentile · FIRST	— 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)

Add an explicit cancel_delayed_work_sync() after brcms_del_timer() to guarantee that any in-flight callback has completed before the timer structure is freed.

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/050d2486e8ed2c0a23b87249ccd23e8072721391	Additional reference	git.kernel.org/stable/c/10eeb0b29fd7f52487c9ae573e8d79c210a0095d
Additional reference	git.kernel.org/stable/c/1edb3ddd261e973a4d577c0547e63bfa25a8170d	Additional reference	git.kernel.org/stable/c/1eeca1d5e0920fbdad6449768fd2d4364e714180
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98196	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93124
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98196		

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