

CVE-2026-98702

Microsoft wifi: mac80211: reject invalid 320 MHz CSA bandwidth

In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: reject invalid 320 MHz CSA bandwidth The HT/VHT channel definition validator can receive a 320 MHz bandwidth indication from a received CSA frame on a non-6 GHz link. It warns for this unsupported width but continues with an uninitialized vht_operation.chan_width, which is then read by ieee80211_chandef_vht_oper(). With panic_on_warn enabled, this lets a received frame panic the kernel.

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)

Reject the channel definition before entering the VHT operation conversion. This preserves the existing CSA fallback while avoiding both the warning and the uninitialized read.

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/1892e71aa2e5ee667d87c6e49e3661f5e290303b	Additional reference	git.kernel.org/stable/c/56e236759f0a8dc910c2ae7cd3c161f298ee5794
Additional reference	git.kernel.org/stable/c/79b3ce0d881cd6e5d4d3496b19f5cc5e7089a56c	Additional reference	git.kernel.org/stable/c/cf0ddacce173890407ed3fa50c8ea9b3c0cc0e16
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98702	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103956
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98702		

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