

CVE-2026-98184

Microsoft wifi: mwifiex: prevent authentication frame length truncation

In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: prevent authentication frame length truncation
mwifiex_cfg80211_authenticate() derives the authentication frame length from req->ie_len and req->auth_data_len, both of type size_t, but stores it in a u16. NL80211_ATTR_AUTH_DATA only has a minimum length policy. Since nla_len is a u16, a single attribute can carry up to 65531 bytes of payload, so the sum can exceed U16_MAX before it is assigned to pkt_len.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 12th 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)

The truncated pkt_len determines the skb frame area, while the copy length remains req->auth_data_len - 4, resulting in a heap buffer overflow. For example, with auth_data_len equal to 65510 and no IEs, the sum is 65546. It is truncated to 10 and then reduced by four to 6. The driver appends only six bytes to the skb with skb_put(), but then copies 65506 user-provided bytes into the authentication body. Reaching this path requires CAP_NET_ADMIN in the user namespace owning the network namespace, an up station netdev, and a suitable BSS/SAE authentication request. Compute the length in size_t, reject values that cannot be represented by the firmware's u16 frame length field, and only then assign it to pkt_len.

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/25c45a2075cc00faed45f92a64bb172fb074a2ee	Additional reference	git.kernel.org/stable/c/5747eaa38a7fcad48be2fd910b65008198b2b06c
Additional reference	git.kernel.org/stable/c/877b61a67d5eb3e616478daf3908114b57feff1e	Additional reference	git.kernel.org/stable/c/fa00193eb991f92b007aefe7afb6a7566976dacf
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98184	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93112
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98184		

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