

CVE-2026-98731

Microsoft Bluetooth: btintel_pcie: fix plen overflow in btintel_pcie_rcv_frame()

In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel_pcie: fix plen overflow in btintel_pcie_rcv_frame() plen is u16 and computed as HDR_SIZE + dlen. For ACL/ISO frames dlen is a 16-bit field, so a value >= 0xFFFFC wraps the sum, bypassing the "skb->len < plen" check and letting skb_trim() truncate the packet. Widen plen to u32 so the addition cannot wrap.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 10.6th 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	0.002 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)

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/7dbeb6935ac331b0cba6c41cabd8e9d02d5f64ea	Additional reference	git.kernel.org/stable/c/b2cb5ea1dc8cf829816370fc1399e6a1d2d1bca9
Additional reference	git.kernel.org/stable/c/c3a3842c109ac130c6db3aa0014cc8cd344928ad	Additional reference	git.kernel.org/stable/c/c3b5e6da4ba6485bffd9753d8339c28855207aa
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98731	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103816
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98731		

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