CVE-2026-98296

Microsoft Bluetooth: btintel_pcie: validate TX skb length in send_sync

In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel_pcie: validate TX skb length in send_sync btintel_pcie_prepare_tx() copies skb->len bytes into a fixed BTINTEL_PCIE_BUFFER_SIZE (4096) DMA slot via an unchecked memcpy. Oversized packets are currently rejected only in btintel_pcie_send_frame(); any future caller of btintel_pcie_send_sync() would silently overflow the DMA buffer. Add the bounds check in btintel_pcie_send_sync() itself, right before skb_push() and the DMA copy.

EVRS	CVSS	EPSS	CISA DEADLINE
0/100 Informational priority	— Not scored	0.002 10.1st 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
Ransomware	Ransomware association unavailable
EPSS	0.002 probability
CVSS	CVSS base score unavailable
Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
KEV recency	CISA KEV listing date unavailable
Pre-patch disclosure	Disclosure status 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/4b837ebd0ea21ae5cc26f02dc042edc6fe7b46b9	Additional reference	git.kernel.org/stable/c/84f353256e170dc4865d45007d1bc446ed566da7
Additional reference	git.kernel.org/stable/c/c298a61e18029401486c40298a50fbeea7e7b663	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98296
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93281	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98296

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