

CVE-2026-98601

Microsoft Bluetooth: btintel_pcie: validate device-supplied DMA indices

In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel_pcie: validate device-supplied DMA indices
In btintel_pcie_msix_rx_handle(), the driver processes RX completion descriptors (urbd1) written by the PCIe device into DMA-coherent memory. urbd1->frbd_tag (a 16-bit field fully controlled by the device firmware via DMA) is used directly as an array index into rxq->bufs[] without any bounds check.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9.3rd 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)

rxq->bufs[] has only BTINTEL_PCIE_RX_DESCS_COUNT (64) entries, while frbd_tag can be any value 0-65535. A malicious or malfunctioning device can write an out-of-range frbd_tag, causing the driver to dereference an out-of-bounds data_buf pointer. Additionally, cr_hia is read from a DMA-shared index array also writable by the device; if the device sets cr_hia >= rxq->count, the while-loop never terminates because cr_tia is wrapped via modulo rxq->count and can never equal an out-of-range cr_hia. Add bounds validation for cr_hia and frbd_tag in the RX path, and cr_hia in the TX path. Log invalid values with bt_dev_err before returning.

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/37a11129345337efd6eef8e62b03b6348cd0dd8b	Additional reference	git.kernel.org/stable/c/8ec5838a35b03ac0cf3602452a369898051ffaf9
Additional reference	git.kernel.org/stable/c/b29b70bfa12133423924fcd0327c19a802f7e368	Additional reference	git.kernel.org/stable/c/f42cd95e679d5b78611cd2208cd1c41ad0045ffa
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98601	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103646
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98601		

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