Wireless Interception of Functional Neuroimaging Transmissions

A. C. Buglione

CVE-2026-2671 is a security vulnerability which results in unauthorized interception of functional near-infrared spectroscopy (fNIRS) sensor data transmitted by the Mendi neurofeedback headset. The core issue is that neural activity data is sent over the air in cleartext, with no encryption applied at any layer of the communication stack.

An attacker positioned within Bluetooth Low Energy (BLE) radio reception range can passively sniff the device's data streams using widely available wireless analysis hardware, such as the Nordic nRF Sniffer application or a modified smartphone. Once captured, these data streams can be decoded to reconstruct the user's hemodynamic response signals, effectively allowing an observer to visualize prefrontal cortex activity in real time without the user’s consent or knowledge.

The attack requires only passive presence within broadcast range and can be carried out without any physical interaction with the target device. No pairing, authentication, or active probing is necessary. Because the interception is strictly passive in nature, it is entirely undetectable by both the user and the client application, leaving no forensic artifacts or evidence of data exfiltration on the device or its associated software.

The root cause of this vulnerability is the failure to enforce secure BLE pairing mechanisms or implement application-layer encryption during data transmission of fNIRS measurements. This omission renders all sensor data accessible in cleartext to any nearby observer with the capability to monitor traffic in the 2.4 GHz ISM band.