Covert Manipulation of Pulsed Electromagnetic Field Characteristics

A. C. Buglione

CVE-2026-2756 is a security vulnerability in the Bluetooth Low Energy (BLE) implementation of the OmniPEMF NeoRhythm pulsed electromagnetic field (PEMF) device. Due to the absence of appropriate encryption and access controls, an attacker within BLE range can inject control signals in real-time, allowing for the unauthorized manipulation of neurostimulation session parameters and introducing a direct physical risk to the user.

The device does not employ BLE pairing, authentication, or encryption mechanisms. The Generic Attribute Profile (GATT) characteristics used to manage the device are openly accessible. Consequently, establishing a connection and writing data to the device does not require authentication tokens, bonding, or PINs, eliminating the need for complex attacks such as connection jamming or cryptographic cracking.

Because the interface is completely open, a third party can directly write arbitrary values to the unprotected BLE control characteristics. Using targeted exploitation frameworks, an attacker can seamlessly inject malicious control signals in real-time to alter active PEMF therapy parameters, including stimulation intensity, frequency, duration, and program modes. Forcing the device to operate outside the user's intended parameters presents a safety hazard; delivering unexpected electromagnetic pulses could theoretically induce adverse neurological effects while leaving the user with no indication of the alteration.

The root cause of this vulnerability is the complete lack of encryption and authentication on the BLE interface. Because the control characteristics are openly writable, critical therapy parameters can be exploited with minimal effort. Remediation requires migrating the firmware to utilize BLE Secure Connections (LESC) with properly authenticated pairing, or introducing robust protocol-layer encryption and mutual authentication to ensure only authorized clients can interact with the device.