Spanalytics, LLC
0101001010101010010

Should I Worry About the Bluetooth and Wi-Fi in My Medical Device?

We Are:

- Leaders in the field of wireless cyber security
- Manufacturer of best-in-class IoT analysis tools
- Decades of experience in security audits and penetration testing
- One of the only companies to do deep dive training in IoT Wireless and Cyber Security
- Located in Richmond, Virginia
- A Veteran-Owned Small Business

Could your Medical Devices' Bluetooth leave you vulnerable to attacks?

Discovered Vulnerabities

Spanalytics has perfomed Bluetooth and Wi-Fi evaluations on dozens of medical devices, finding a variety of problems, like:

- ➢ Weak Bluetooth security (Mode 1, Level 1), allowing for passive eavesdropping. Seen on a thermometer, a BP monitor, and a pulse oximeter
- ➢ Sending a malformed packet to a blood pressure monitor caused the device to lock, requiring a power cycle

Identified Bluetooth and Wi-Fi Weakness:

Denial of Service:

Various levels of susceptibility to DoS attacks from remote devices. Additional vulnerabilities can exist when a DoS attack is performed.

SweynTooth and BrakTooth:

Allows unauthorized users to wirelessly crash a device, preventing it from working or allowing access to functions limited to users.

Eavesdropping:

Potential weakness leaving valuable personal information to be listened to via Bluetooth packets, leaving way to things like identity theft

Weak Authentication:

Some devices allow a authentication down-grade attack, like using the Secure Simple Pairing, Just Works Association Model

Buffer or Interger Overflow Error:

Occurs when a variable or memory location is fed a set of data that exceeds the allowed allocation, making it easy to override.

Discoverability:

Always discoverable or is discoverable for "too long". The longer your device is discoverable the easier it is to identify by a hacker.

Connectability:

Always connectable or is connectable for "too long." This can lead to DoS, fuzzing, or other attacks. A unit should also limit the time it attempts to auto-connect to trusted devices.

Home Grown Security:

Some vendors will "roll their own" encryption and/or authentication, resulting in algorithms that have not been peer-reviewed and can be hacked

Weak Bluetooth Encryption:

Does not enforce 128-bit encryption key size or fails to initiate encryption when the connected device does not start encryption

Outdated Firmware:

The medical industries firmwares are constantly evolving to meet the increasing list of vulnerabilites found. With old firmware, patches that have already been released may not be included on your device.

Wi-Fi Weak Encryption:

WEP encryption is allowed, which can be broken

Physical and Mailing Address: 4190 Innslake Dr., Glen Allen, VA, 23060
Phone: (804) 364-1050 **Email:** contact@spanalytics.com **Website:** Spanalytics.com