SECURITY INNOVATION | A BUREAU VERITAS COMPANY

HACKERS○HACK

HH○ MEDICAL DEVICE

Building trust in a software world.

Hacking BLE for Healthcare: Securing Presence, Protecting Patients

PROJECT

Medical Device Security

CUSTOMER CONCERNS

Automated medical devices that connect to hospital networks and cloud services present unique security challenges. In this particular case, the target was an embedded system that allowed hospital personnel to authenticate to workstations by means of Bluetooth Low Energy that performed active presence detection and user tracking. The client was concerned that potential vulnerabilities could allow unauthorized device or workstation control, data tampering, or the exposure of sensitive patient information. The objective was to assess the device's resilience to cyberattacks and ensure compliance with industry regulations.

THE MISSION: WHY WE HACKED IT

Security Innovation was tasked with evaluating the medical device's software, embedded hardware, network connections, and data management practices. The mission was to identify security gaps that could be exploited to compromise patient safety or disrupt medical procedures.

THE BREAKDOWN: WHAT WE FOUND

Our security assessment involved:

- **Network Vulnerability Testing:** Assessed connections to hospital and cloud networks for weaknesses that could allow unauthorized access.
- **Data Integrity Analysis:** Evaluated how patient data was stored and transmitted, focusing on encryption and tampering prevention.
- **Hardware Attack Simulation:** Ubertooth One and NRF51 were used to sniff the BLE traffic between the target components of the customer hardware and application. Gatttool was used to discover, read, and write to available BLE characteristics.
- **Device Control Simulation:** Simulated potential attack scenarios to test if remote control of the device was possible.

KEY FINDINGS INCLUDED:

- **Insufficient Data Encryption:** Found that certain data transmissions were inadequately protected, posing a risk of interception and tampering.
- **Unrestricted BLE Characteristics:** Insecure Bluetooth Low Energy (BLE) settings left the proximity tracking vulnerable to manipulation, enabling unauthorized monitoring of user activity and interference with expected operations
- **Flawed Authentication:** Intercomponent interactions and protocols were insecure, potentially enabling a jamming attack that would circumvent system authentication.
- **Piggybacking Attacks:** MITM on the Bluetooth connection allowed capturing the UUIDs, MAC and other values to add them to another application without consent.
- **Unauthorized Access Paths:** Identified pathways that could allow attackers to gain control over the device or access patient data.
- Regulatory Gaps: Highlighted areas where security measures did not align with industry regulations, impacting compliance.

BY REMEDIATING THESE ISSUES, THE CLIENT WAS ABLE TO:

- **Enhance Data Encryption:** Implement comprehensive encryption standards to safeguard patient data.
- **Secure Network Access:** Close unauthorized access paths and strengthen authentication measures.
- **Achieve Compliance:** Align device security protocols with industry standards to meet regulatory requirements**.**

These improvements significantly increased the security and reliability of the medical device, ensuring patient safety and data protection.