SecurityInnovation®
THE SOFTWARE SECURITY COMPANY

Health Corp
Blood Pressure Monitor 3000
Threat Model

Project:	Health Corp - Blood Pressure Monitor 3000
Document Name:	Threat Model
Customer:	Health Corp
Customer Contact:	Jane Doe <jane_doe@health.corp>
Threat Model Author:	John Doe <jdoe@securityinnovation.com>

SecurityInnovation®
THE SOFTWARE SECURITY COMPANY
Boperating systemTON | SEATTLE
187 Ballardvale St. Suite A202 ●Wilmington, MA 01887● Ph: +1.978.694.1008
getsecure@securityinnovation.com● www.securityinnovation.com

Contact Information

Security Innovation

Business Contact
sales@securityinnovation.com

Technical Contact
John Doe
jdoe@securityinnovation.com

Health Corp

Jane Doe
jane_doe@health.corp

Table of Contents

Executive Summary

Security Innovation will perform a security audit of the Health Corp Blood Pressure Monitor 3000 (BPM3000) clinical device.

Security Innovation reviewed all available documentation, performed exploratory testing, and met with technical leads to build a complete understanding of the BPM3000 system. During each meeting, an understanding of each of the following areas was discussed:

- Features and use cases of the component
- Users of the component
- What data is being consumed and produced by this component
- What data must be protected or is considered sensitive
- If there is an administrative interface, how it is used and how it is protected
- Any existing security controls, reviews, or considerations
- Protocols, libraries, frameworks, or other external components used
- Biggest security concerns as viewed by the teams

Threat modeling is the first step for successful software security audits. The BPM3000 threat model shows the results of a close security analysis of the BPM3000 design. Security Innovation will use this threat model to gather attack vectors and generate test cases for comprehensive security testing of the BPM3000.

The following list summarizes the important points that impact the attack surface of the BPM3000:

- The device has wired and wireless connections to the hospital network
- Firmware updates are only performed over USB
- Data is only stored for 72 hours and deleted after 12 hours of being powered down
- The device accepts external HID input
- The device runs a Windows 7 embedded operating system
- Authentication and authorization controls are used to restrict access to various functionality

The top threats for malicious attack are:

- Uploading malicious firmware to the device
- Unauthorized access to key health data during transmission or at rest
- Unauthorized access to proprietary algorithms and intellectual property

Introduction

Threat modeling is a necessary step to create actionable security test plans and to properly understand the security footprint of the system. Security Innovation has created a Threat Model to analyze and gather all possible avenues of attack.

The Threat Model is the result of a methodology to determine the primary threats to the system being evaluated. Threats are potential attacks on the assets of the system which are inherent to the system that may or may not actually be possible. A threat does not imply a vulnerability. By analogy, if one keeps large sums of money in a safe, there is the threat that an attacker could steal the money. This threat is inherent in money storage and does not imply a specific vulnerability in the safe that would allow an attacker to realize it.

By systematically enumerating how the assets of the system could potentially be compromised by an attacker, the following phases of the evaluation can determine which threats can be realized by attackers utilizing existing vulnerabilities.

The attack vectors identified in the Threat Model will be used to generate test cases in the security test plan along with the conditions and steps required to execute each of them.

The BPM3000 clinical platform is a modular medical device that provides clinical care blood pressure monitoring services for bedside hospital environments. The device interfaces with several external sensor modules connected to patients. The device runs the Windows 7 embedded operating system which hosts Health Corp's proprietary code.

Threat Model Creation Methodology

The Security Innovation threat modeling methodology comes from years of experience threat modeling to find the most impactful and actionable threats in a system. It is designed to quickly assess each role, asset, component, and activity to understand the most common and highest priority threats to the system.

Threat modeling consists of the following steps:

1. Understand architecture and security requirements
2. Identify assets, roles, and system components
3. Build an activity matrix and define the related rules
4. Identify threats that put assets at risk
5. Assign related components to each threat
6. Identify conditions under which a threat may be realized

Once the threat model is complete it is used to:

1. Guide Design Reviews which can highlight early application flaws that can be costly to fix later
2. Highlight high-impact areas for a Code Review to help create Code Review Objectives documents
3. Create a Test Plan that can be used to test for the presence of the threat using black box methodology
4. Choose appropriate mitigations and responses to any realized threats

System Decomposition

In this section, Security Innovation will enumerate each component of the system that influences the Threat Model.

These features include the following:

- **Assets** - Any high value information the attacker may target.
- **Roles** - Each different level of privilege on the system a malicious user may acquire.
- **Components** - The physical pieces of the system that may hold assets, validate roles, or connect other components.

Assets

- **Application User Credentials** - The credentials used to unlock features, change features, and administer various aspects of the device.
- **Windows Account Credentials** - The credentials for the underlying operating system user accounts.
- **Patient Health Information** - The health information entered by the hospital worker and information gathered by the device over the course of its use.
- **Application Binaries** - The proprietary software, algorithms, and intellectual property on the device.
- **Diagnostics Logs** - The various logs used to provide diagnostic and debugging information gathered during faults or runtime.

Roles

- **Anonymous** - An unregistered user on the system. Nurses and doctors fall into this category.
- **Technician** - An IT employee that configures the device features and subsystems.
- **Administrator** - A system administrator that updates firmware or can administer and configure the underlying operating system.

Components

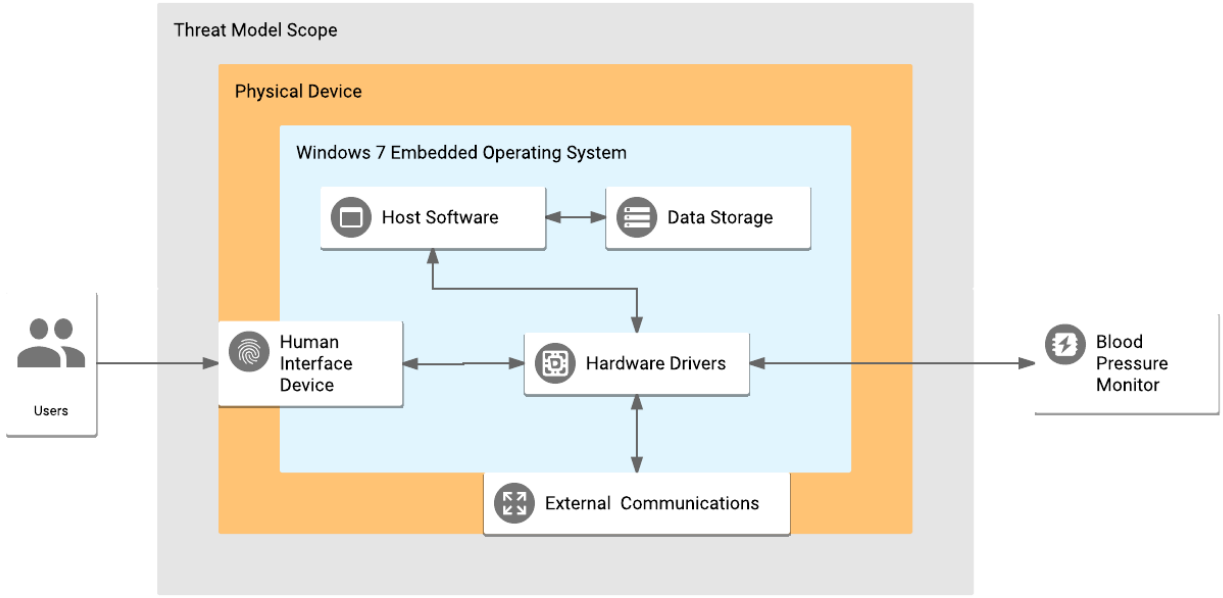
Each component in the following table may hold zero or more assets. The component may store, process or transmit data on the system.

Component Name	Type	Description
Host Software	Thick Client	This is the host software running on the device that communicates with the sensor control modules, gathers and records data, and renders and controls the user interface.
Operating System	Operating System	This is the Windows 7 Embedded operating system that manages the host software, hardware drivers, data storage, and other computing components.
Hardware Drivers	Firmware	These are the drivers that allow the software and operating system to communicate with and control connected hardware components.

Component Name	Type	Description
Physical Device	Device	This is the physical device (housing, screen, ports, buttons, and electronics) that houses all the software and connections to the sensor control modules.
Data Storage	Database	This is the data storage mechanism used to record information gathered and processed by the device.
External Communications	Network	This is the component covering communication with external systems via one-way serial broadcast or two-way network communication.

Component Diagram

The following component diagram illustrates the relationship between each component in the system. Components inside the grey box are covered in the table above, other components are supporting or adjacent components and fall outside of the scope of this assessment.



Activity Matrix

The following Activity Matrix shows the interactions between each asset and role in the BPM3000 system.

Asset	Action	Role: Anonymous	Role: Technician	Role: Administrator
Application User Credentials	**Create**	Never	Never	Always
	Read	Never	Never	Never
	Update	Never	Never	Always
	Delete	Never	Never	Always
Windows Account Credentials	**Create**	Never	Never	Always
	Read	Never	Never	Never
	Update	Never	Never	Always
	Delete	Never	Never	Always
Patient Health Information	**Create**	Always	Always	Always
	Read	Sometimes[1]	Sometimes[2]	Sometimes[2]
	Update	Always	Always	Always
	Delete	Always	Always	Always
Application Binaries	**Create**	Not Applicable	Not Applicable	Not Applicable
	Read	Never	Never	Always
	Update	Never	Always	Always
	Delete	Never	Never	Always
Diagnostics Logs	**Create**	Never	Never	Never
	Read	Never	Always	Always
	Update	Never	Never	Never
	Delete	Never	Always	Always

The following rules apply to the items labeled "Sometimes" in the Activity Matrix above:

- Sometimes[1] – This user can perform this task, but only for data immediately available on the UI.
- Sometimes[2] – This user can perform this task, but only for data stored over a 72-hour window.

Threat Tree Information

The following section contains the complete list of threat trees developed for the BPM3000. Each threat includes the priority and a description of the potential threat. Beneath each threat header is the component that is affected, the sub bullets under each asset represent attack scenarios that could make the threat possible.

The following list represents theoretical threats against the system. A test plan will be created using these threat trees. The individual tests against the live system will show or disprove the existence of each threat.

Threat Priority

The priority rating for each threat is based upon the perceived damage impact to the asset.

- **P1:** Significant system compromise via elevation of privilege, disclosure of sensitive assets, or tampering with/repudiation of critical system activities.
- **P2:** Server-side or widespread denial of service, disclosure of implementation detail or less sensitive assets, non-critical repudiation/logging issues.
- **P3:** Client-side or minor denial of service, alteration of user experience without affecting functionality, minor information disclosures.

Legend

Target Component

- Exploitation Circumstances
  - *Priority: Threat (STRIDE Type)*

Threat Trees

Threat List

Below is a list of the threats to the assets contained in the system. This list is generated by using the access matrix, threat priority key, and STRIDE categories. The threats are then mapped to components and vulnerabilities in the next section. A vulnerability in a component would cause a threat to be realized.

- *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
- *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
- *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
- *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
- *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
- *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
- *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
- *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
- *P1: Application binaries can be updated by an unauthorized user (Tampering)*
- *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
- *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
- *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
- *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
- *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*

Threat Tree

Host Software

- Insufficient authentication and authorization controls for access to sensitive data locations
    - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
    - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
    - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
    - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
    - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure handling of input allowing for memory corruption, leading to arbitrary code execution

- *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
- *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
- *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
- *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
- *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
- *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
- *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
- *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
- *P1: Application binaries can be updated by an unauthorized user (Tampering)*
- *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
- *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
- *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
- *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
- *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
- *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

- Utilizing unsigned binaries and libraries
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*

  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure database query functions allowing for malicious database reads or writes
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure firmware update process allowing for malicious firmware overwrite
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Host software not sufficiently locked down to prevent access to underlying operating system
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*

-
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure handling of input allowing for memory leak
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
- Vulnerable business logic functionality allowing unintended manipulation of application functionality
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

Operating System

- Known vulnerable operating system or default services susceptible to public exploits
    - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
    - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
    - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
    - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
    - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
    - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
    - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure remote administration controls allowing remote access to the operating system
    - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
    - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
    - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*

- *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
- *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
- *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
- *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

- Use of weak default user account credentials
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure Window's services allowing for local privilege escalation
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*

  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure permissions on application files or directories containing application files
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

Hardware Driver

- Insecure handling of input allowing for memory corruption, leading to arbitrary code execution
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*

  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*
- Insecure handling of input allowing for memory leak
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*

Physical Device

- Missing anti-tampering mechanisms allowing for tampering with electronics hardware
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

- Insecure boot process allowing for boot process hijacking
    - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
    - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
    - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
    - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
    - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
    - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
    - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

Data Storage

- Insecure access controls for critical data storage locations
    - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
    - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
    - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
    - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
    - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
    - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*

- *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
- *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
- *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
- *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
- *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

- Missing or insecure encryption/signing of sensitive data at rest
  - *P1: Authentication credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Authentication credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Authentication credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Windows account credentials can be created by an unauthorized user (Elevation of Privilege)*
  - *P1: Windows account credentials can be read by an unauthorized user (Information Disclosure)*
  - *P1: Windows account credentials can be updated by an unauthorized user (Tampering)*
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be read by an unauthorized user (Information Disclosure)*
  - *P1: Application binaries can be updated by an unauthorized user (Tampering)*
  - *P2: Windows account credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P2: Application binaries can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Authentication credentials can be deleted by an unauthorized user (Denial of Service)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*
  - *P3: Diagnostic logs can be deleted by an unauthorized user (Denial of Service)*

External Communications

- Insecure transmission of patient health information over the network
  - *P1: Historical patient health information can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be read by an unauthorized user (Information Disclosure)*
  - *P3: Diagnostic logs can be updated by an unauthorized user (Tampering)*