IoT Security Assessment Report for

**{pentest\_name}**

Contents

[1 Executive Summary 4](#_Toc24452207)

[2 Introduction 5](#_Toc24452208)

[2.1 Scope 5](#_Toc24452209)

[2.2 Methodology 5](#_Toc24452210)

[3 Timeline 6](#_Toc24452211)

[4 Vulnerabilities & Security Concerns 7](#_Toc24452212)

[4.1 Application Vulnerabilities 7](#_Toc24452213)

[4.2 Infrastructure Vulnerabilities 7](#_Toc24452214)

[4.3 Process Vulnerabilities 7](#_Toc24452215)

[5 Other Findings 9](#_Toc24452216)

[6 Appendix A 10](#_Toc24452217)

[6.1 Vulnerability Risk Rating 10](#_Toc24452218)

[6.1.1 Risk Level 10](#_Toc24452219)

[6.1.2 **Critical (GIA Major)** 10](#_Toc24452220)

[6.1.3 **High (GIA Major)** 10](#_Toc24452221)

[6.1.4 **Medium (GIA Non-Major)** 11](#_Toc24452222)

[6.1.5 **Low (GIA Non-Major)** 11](#_Toc24452223)

# Executive Summary

{@executive\_summary}

Below is a summary of the findings, vulnerability score, and next steps for remediation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability** | **Effort** | **Impact** | **Vulnerability Score** | **Recommendation on Remediation** |
| {#snapshot}{name} | {effort} | {impact} | **{score}** | {@remediation}{/snapshot} |

Informational findings are listed below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability** | **Effort** | **Impact** | **Vulnerability Score** | **Recommendation on Remediation** |
| {#fyiSnapshot}{name} | - | - | **{score}** | {@remediation}{/fyiSnapshot} |

# Introduction

The testing was conducted simultaneously by the following team members: {team\_members}. This section describes the scope and methodology used by the team to conduct this assessment.

## Scope

The following components are within the scope of this project.

{@scope\_description}

## Methodology

|  |  |
| --- | --- |
| White-box Testing | * Analyze internal documentation of the systems in scope. * Analyze source code of the applications and firmware in scope. * Use development hardware devoid of some of the security features. * Consult observations with the development team and seek their feedback. |
| Firmware analysis | * Analyze the firmware in search of hardcoded credentials, misconfigurations, coding errors, etc. |
| Network traffic analysis | * Record and analyze the network traffic exchanged by the devices and applications. * Recreate network-level interactions in the lab environment. Impersonate each side of the interaction and look for protocol-level vulnerabilities. |
| Radio traffic analysis | * Record and analyze communication exchanged over the radio (e.g. Bluetooth). * Recreate radio interactions in the lab environment. Impersonate each side of the interaction and look for protocol-level vulnerabilities. |
| Initial setup analysis | * Analyze the initial device onboarding process. |

# Timeline

|  |  |
| --- | --- |
|  | **Details** |
| {#tl\_entries}{tl\_date} | {@tl\_description}{/tl\_entries} |

**Note:** All times are Eastern Time (EST/EDT)

# Vulnerabilities & Security Concerns

Listed below are the vulnerabilities and security concerns discovered during the assessment. These are considered significant and steps should be taken to address them.

## Application Vulnerabilities

|  |  |
| --- | --- |
| {#appFindings}{name} | *{score}* |
| **Description**  {@description}  {#attachments}  {%dataURL}  ***{label}***  {/attachments}  **Components Affected:**{#hosts}  {.}{/hosts} | |
| **Recommendation/Remediation** | |
| {@remediation} | |
| {/appFindings} | |

{^appFindings}None Found.{/appFindings}

## Infrastructure Vulnerabilities

|  |  |
| --- | --- |
| {#infFindings}{name} | *{score}* |
| **Description**  {@description}  {#attachments}  {%dataURL}  ***{label}***  {/attachments}  **Components Affected:**{#hosts}  {.}{/hosts} | |
| **Recommendation/Remediation** | |
| {@remediation} | |
| {/infFindings} | |

{^infFindings}None Found.{/infFindings}

## Process Vulnerabilities

|  |  |
| --- | --- |
| {#proFindings}{name} | *{score}* |
| **Description**  {@description}  {#attachments}  {%dataURL}  ***{label}***  {/attachments}  **Components Affected:**{#hosts}  {.}{/hosts} | |
| **Recommendation/Remediation** | |
| {@remediation} | |
| {/proFindings} | |

{^proFindings}None Found.{/proFindings}

# Other Findings

Listed below are informational findings and security concerns discovered during the assessment. These are considered insignificant and would often not require any immediate action.

|  |  |
| --- | --- |
| {#fyiFindings}{name} | *{score}* |
| **Description**  {@description}  {#attachments}  {%dataURL}  ***{label}***  {/attachments}  **Components Affected:**{#hosts}  {.}{/hosts} | |
| **Recommendation/Remediation** | |
| {@remediation} | |
| {/fyiFindings} | |

{^fyiFindings}N/A{/fyiFindings}