.

Security Assessment

Samsung Gear S3 Frontier

Company name: Fontys

Date: 18.11.2020

Colophon

|  |  |
| --- | --- |
| **Label** | **Gegevens** |
| Client | Fontys |
| Autor | Thomas van Heel en Joël Adams |
| Status | Review |
| Classification | Confidention |

Version history

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Changes** |
| 1.0 | 18-11-2020 | Setup and fill with content |
| 2.0 |  |  |

Review

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Reviewed by** |
| 1.0 | 20-11-2020 | Merlijn Vermeer |

## 

**Chapter 1**

**Management Summary**

Fontys students of semester 7 have performed a time-limited penetration test of the Samsung Gear S3 Frontier smartwatch.This has been done in our own environment.

Our impression of the security level of this smartwatch is quite positive. For example, the smartwatch doesn’t have any unnecessary open ports. Besides that, there wasn't any security risk in this IoT system.

Although we found the OS version of the smartwatch. This version had a lot of vulnerabilities, but only one of them had a well-described PoC. However, there wasn’t any success on this exploit.

In this report you can find all the details of our research and findings, this also includes all technical advice.

1.1 Risks

The graph below shows the identified findings by each category of the CVSS:

1.2 Overview findings

The findings are sorted based on the CVSS classification. If more information is needed, it can be seen at [3.2 Analysis](#_vf3fa0h49e3n).

**Table of Contents**

[**Chapter 2**](#_9ebguro5h6st) **6**

[**2.1 Research question**](#_l5zynsppyp6s) **6**

[**2.2 Scope**](#_gm2gnfqavhfj) **6**

[**3.1 Approach**](#_ubioixhhvus6) **7**

[3.1.1 General](#_m75qw8rytc2y) 7

[3.1.2 Web](#_kd6p7povjkss) 7

[**3.2 Analysis**](#_vf3fa0h49e3n) **7**

[**Chapter 4**](#_l9rj5ydqhqo4) **8**

[**4.1 Conclusion**](#_cfnbf0p1jr4l) **8**

[**4.2 Advice**](#_b282lo8radkt) **8**

[**Appendix A**](#_x9pd8qhgsqbk) **9**

# Chapter 2

**Your request**

Nowadays people use more IoT devices than before, those differ from big Iot systems to little applications. One of the IoT systems is the smartwatch. Those systems have a lot of sensitive information, such as agenda, contacts and location. For sure that information needs to be sent and stored in a secure way.

The stakeholder of this project is Fontys, in specific: Casper Schellekens. He is the contact to talk with if there are any questions and present our findings to them.

This project is used in a larger project, creating IoT guidelines. The findings from this pentest will be used to create guidelines to make safer and more secure IoT appliances/systems.

# **2.1 Research question**

The system that is going to be tested is everything according to the smartwatch, such as back-end, traffic and services. The goal is to try and find some general vulnerabilities and write down what the findings are. For example, there will be searched for *password storage*, *broken authentication* *and* *privilege escalation*.

# **2.2 Scope**

The scope of the project is the smartwatch, included back-end, services and traffic .

**Chapter 3**

Our Findings

# **3.1 Approach**

We connected the smartwatch to a router and made it reachable, so we could pentest it. We followed the kill-chain:

1. Reconnaissance
2. Intrusion
3. Exploitation

## **3.1.1 General**

To test everything within the scope we did a form of scanning and exploitation after.

## **3.1.2 Web**

Testing was done on a server that was accessible to everyone in the group. The tools that were used are mostly the same tools we use in Kali Linux for other pentests. Among these are:

* Nmap
* Tizen studio

# **3.2 Analysis**

Below is a description of every problem found. Listed are the compromised systems and a quick explanation of the exploit. The more technical explanation is in the appendix to provide a better understanding of what went wrong and what could be better.

1. **Broken access control**

* If a hacker can analyze the D-Bus of the smartwatch, he can see with interface and methods are publicly accessible, through these methods the hacker can take over the smartwatch. For example, download sensitive data and take screenshots.

This is because the Tizen OS version 4.0.0.4 is vulnerable. At least the D-Bus of this OS is vulnerable.

## **Chapter 4**

**Conclusion and advice**

The pentest concluded with no successful exploits.

# **4.1 Conclusion**

There are no findings at all for this IoT system. Although there is an outdated Tizen version(v4.0.0.4). This version is vulnerable and this is the attack vector we saw in this system. We couldn’t exploit it, because the Tizen Studio application couldn’t connect to our smartwatch/smartphone.

# **4.2 Advice**

Because the Operating system of the watch (Tizen) was outdated, it was the only critical attack vector we had. It is advisable to check the watch (or phone it is connected to) for updates for either the app on the phone or the watch itself.

## **Appendix A**

**Technical Findings**