Federal Office
for Information Security

Security assessment of wearable devices with medical functionalities (SiWamed)

Cybersecurity Assessment

Document history

Version	Date	Editor	Description
1.0	28.11.2023	BSI Referat DI24, eShard, eesy-innovation	Initial creation

Table 1: Document history

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-DI24@bsi.bund.de
Internet: https://www.bsi.bund.de

Acknowledgements

This report has been developed in collaboration with the Federal Office for Information Security (BSI), represented by the project managers Mrs Mayer and Mr Kleinmanns (Referat DI 24). The participating project partners eShard GmbH and eesy-innvovation GmbH would like to thank the project managers for their competent and critical support of this project.

The project benefited from a close, goal-oriented and trustworthy collaboration between all parties and participants involved. A special thanks is owed to (in alphabetic order): Jochen Arold (eesy-innovation), Hlib Budylo (eShard), Christian Kleinmanns (BSI), Anna Lackner (eesy-innovation), Alexandra Mayer (BSI), Florian Mommertz (eShard), Thilo W. Pannen (eShard).

Table of Contents

Index of tables

Index of pictures

1 Introduction

Digitization takes place everywhere and is permeating state, economy, and many areas in society. It often contributes to a better life and offers innovation resulting in more comfort or increase of efficiency. At the same time, the growing connectivity of electronic devices, household appliances and other everyday items carries new risks and offers new attack surfaces to criminals and bad actors.

In recent years, consumers have been increasingly using sensors in wearables devices (in short: wearables) to keep track of their health and fitness status. Wearables are small computer systems that are worn directly on the body. Today, it is commonplace to measure or calculate heart rate, blood pressure, blood glucose levels, blood oxygen content, sleep patterns or calorie consumption, among others. Wearables often feature various interfaces, allowing integration into networks. They are also commonly linked and connected to mobile applications (apps) for processing, analysis and management of sensitive data collected and keeping statistics.

Although wearables and their components are passive devices, they may impact the behaviour and health of users. For example, an attack on the sensor or the communication channel used by the wearable could lead to an incorrect judgement of one's true health status, which in turn could result in potentially false and dangerous self-medication. Real-world examples are:

- an incorrect measurement or false display of blood glucose levels prompting the intake of blood sugar-lowering medication;
- an incorrect measurement or false display of blood pressure leading the user to apply medication for blood pressure reduction;
- an incorrect measurement and false display of the blood oxygen content results in dispensation of oxygen.

However, the distinction between a medical device (regulated and subject to an approval process) and a wearable device for personal use (unregulated and not subject to an approval process) is not always easy to consumers and end users. Similar with medical devices, a malfunction of a wearable, either caused by a technical glitch or a targeted attack, can harm recovery of a patient who adjusts his medication to the information provided by the wearable.

Vulnerabilities in devices that process health and fitness data pave the way for a new form of personalised cybercrime. It is conceivable that individuals known to be users of wearables become victims of targeted attacks. It is also imaginable that targeted attacks could be applied to harm the recovery of patients who adjust their medication based on sensor data.

Everyone gaining access to data gathered by wearables could use it for criminal activities, for example in conjunction with theft of identity. Additionally, data could also be misused for a practice called "doxing", where a person's data is obtained with the specific intent of publishing it on the internet and harming an individual. For example, disclosing sensitive data could lead to severe damage to a person's image and reputation. Similarly, individuals whose data has been stolen could be extorted through the threatened disclosure of sensitive data or information.

It is therefore important that users of wearables can rely on their devices with confidence and are aware of the risks of using them.

The project "Security of wearable devices with medical functionalities (SiWamed)" was set up by the Federal Office for Information Security (BSI) to conduct a cyber-security assessment of wearable devices equipped with sensors for recording health data and available on the German market. The project aimed to provide an overview on devices that offer, at a minimum, sensor technologies used for measuring pulse and blood oxygen content. Ideally, a wearable would additionally offer sensor technology supporting creation of an electrocardiogram (ECG).

This study at hands was commissioned with the following objectives:

- assessment of the use of wearables and connected components (mobile app, standalone app, web app or cloud app), and the security and protection of the collected health data,
- identification of potential IT vulnerabilities in wearables and/or components, and
- raising awareness among users, the public and manufacturers.

It places an emphasis on data security and assesses the technical measures implemented regarding their ability to protect and maintain the integrity, confidentiality, and availability of the data. To achieve this, the testers developed customized test plans and analysed the wearables and their related components for vulnerabilities, simulating a technically advanced and smart attacker with limited efforts.

The study begins with a definition of wearables, which is important for the market analysis that follows. The market analysis examines the wearable devices available in Germany and categorises them into four segments: smartwatches, basic watches, fitness trackers and smart rings, based on their respective characteristics. The most relevant wearable devices in each of these four categories were selected for further analysis.

The test procedures for each component of a wearable, i.e., the wearable device carrying the sensors, the mobile app and backend, as well as the test results (anonymised) are presented. The test results are the basis of the cyber security review, summarising the results of the study.

The study concludes with a high-level view on the security status of the wearable devices and their components.

2 Project partners

This study was prepared by the project partners eShard and eesy-innovation on behalf of and in cooperation with BSI, represented by department DI 24, responsible for cyber security in the public health and financial sectors.

2.1 Federal Office for Information Security

As the national cyber security authority, the Federal Office for Information Security (BSI) is responsible for digital information security for the government, businesses and society through prevention, detection, and reaction. The BSI is the federal cyber security agency and the chief architect of secure digitalisation in Germany. Since it was founded in 1991, the BSI has developed into a cross-departmental competence centre for information security issues, with technical expertise that is recognised nationally and internationally.

Digitisation is crucial for Germany's future success. And a prerequisite for successful digitisation is information security: information security and digitisation are inseparable. The BSI deals with digitisation applications where risks could occur and examines how they can be made calculable and controllable. Its distinctive internal and external networking allows the BSI to bundle know-how in the areas of prevention, detection, and response, to analyse information security topics technically and to produce targeted support for different target groups in government, business, and society. The integrated value chain of the BSI ranges from defence and analysis of cyber-attacks through consulting and certification, and right to the development of security recommendations, best practices, and standards.

With the increasing spread of new technologies like artificial intelligence, 5G or smart home/smart factory, the question of trustworthiness is never far away. Trust is created, among other things, through security, which is why the BSI addresses this issue holistically. To increase the information security of new technologies, part of the BSI remit is designing practice-oriented security requirements, standards, and recommendations for action. As the central certification and standardisation body in Germany, the BSI assumes responsibility in this area too. The BSI is also contributing significantly to the success of the major digitisation projects of our time, such as by developing security criteria for smart electricity meters as part of the energy revolution. The BSI is supporting the securing of a digitised transport infrastructure that allows autonomous driving. The BSI has helped to design and certify the essential security anchors of the electronic health card and has established internationally recognised requirements for securing cloud infrastructures. In doing so, the BSI uses its know-how as a national competence centre in the field of cryptography. The BSI also focuses on the information security of new, disruptive technologies, like artificial intelligence or 5G infrastructures.

Within the framework of digital consumer protection, the BSI pursues a holistic approach: manufacturers of digital products are encouraged to bring them to market with appropriate security features. At the same time, the BSI raises the risk awareness of consumers, giving them the confidence needed to act and reduce risks on their own. Therefore, consumers benefit from practical information and recommendations aimed at the lay person, which helps improve the society’s resilience against cyber threats.

Contact:

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Referat DI 24 - Cyber-Sicherheit im Gesundheits- und Finanzwesen

Godesberger Allee 185-189

53175 Bonn

E-Mail: referat-DI24@bsi.bund.de

WWW: https://www.bsi.bund.de

2.2 eShard

eShard was founded in Bordeaux/France in 2015 by two cyber security experts. Today, eShard is an ambitious, growing and internationally oriented company with more than 50 employees located in France (Pessac, Marseille, Macon) and Germany (Bonn).

Today, eShard stands for testing of security of

- ICs, SoCs, Firmware and crypto functions, and
- Operating systems, applications, mobile apps and backend systems (applications and infrastructure).

It is eShard's passion and mission to support its customers with provision of expertise, tools and services to realise the best level of security in their products and solutions.

Since intelligent tools play a significant role, eShard has developed its innovative tools esDynamics, esFirmware, esReven and esChecker to support developers and experts in their daily work and the security analysis. In addition to the development of tools, eShard supports its customer with expertise and consultancy services related to the security and risks analysis in mobile and IoT ecosystems.

In 2021, eShard founded a German subsidiary with a focus on security and penetration testing of backend systems, i.e. APIs, web applications, active network components, cloud applications and infrastructures as well as special systems (e.g. ATMs, IoT devices, healthcare devices), and the provision of related services.

Contact:

eShard GmbH

Beethovenallee 21

53173 Bonn

E-Mail: contact@eshard.com

WWW: https://www.eshard.com/

2.3 eesy-innovation GmbH

eesy-innovation GmbH (EESY) is a research and engineering service provider for full-cycle hard- and software development. The company designs, develops and implements customised IoT solutions for use in different sectors, e.g. industry, healthcare, sports and education, smart home and others. EESY offers a broad range of API, web- and microservices for end-to-end-solutions for sensor measurement data collection, analysis, real-time data visualisation and remote controlling of IoT solutions.

With an international team of 30 full time employees and approx. 20 freelancers in Germany and Spain, EESY supports multiple recognized business customers in various application domains and sectors. Since its foundation, EESY has participated in more than 50 funded research projects and has filed approx. 25 patents.

Contact:

eesy-innovation GmbH

Leipziger Str. 16

82008 Unterhaching

E-Mail: info@eesy-innovation.com

WWW: https://www.eesy-innovation.com

3 Wearables

This chapter begins with a definition of a wearable or wearable device to which the subsequent market analysis and the selection of devices refer.

3.1 Definition

Since the term “wearable” has not been uniformly defined, a definition that will be used in the context of the market survey is presented. This definition is provided by Gabler Wirtschaftslexikon [8] and outlines a wearable as

> *“[...] computer technology worn on the body or on the head. It is a manifestation of ubiquitous computing, the omnipresence of data processing and part of the internet of things. Another term used is wearable technology or wearable computer. The primary purpose is typically to assist an activity in the real world, for example the provision of (additional) information, statistics or instructions.”*

In accordance with this definition, wearables are available in a broad variety and in many form factors, for example as

- smartwatches,
- fitness trackers,
- data or augmented reality glasses,
- EKC sensors,
- smart rings,
- intelligent plasters,
- chest straps,
- fall sensors,
- arm cuffs,
- people tracking,
- finger sensors,
- smart clothes with embedded sensors, or
- hearing aids with enhanced functionalities.

The functionality of wearables varies widely, ranging from e.g., a simple fitness tracker with a step counter to complex sensors that are commonly used in medical devices, such as electrocardiogram (ECG) devices. Examples of wearables include:

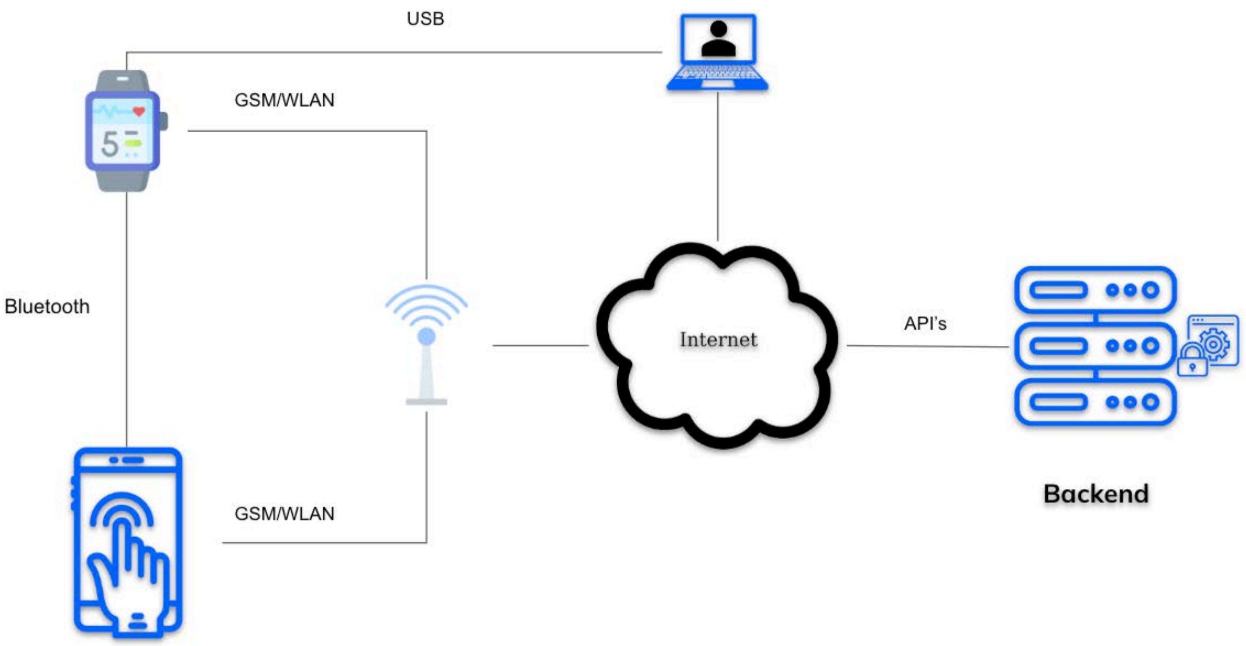
- intelligent jewellery, e.g., rings, cuffs, watches, and stickers. Such small devices usually operate in combination with a mobile app serving as the display and user interface;
- sensors worn directly on the body’s surface for collection and transmission of biological and health data;
- fitness trackers, often designed as wrist bands or belts, and monitoring physical activities or vital parameters. Trackers could be connected and paired with mobile apps to store and process data, and provide feedback to the user;
- smart clothes with embedded technology, allowing e.g., to track the fitness or health status, interact with mobile apps on smartphones or other peripherals, or change its characteristics according to personal preferences, activities or environmental conditions;

- AR headsets that add digital information into the user's environment, and Mixed Reality headsets that connect physical reality with digital content, so that interaction between physical world and virtual objects is facilitated. (VR headsets are on the opposite end of the virtualization spectrum, and fully replace the user environment by digital information);
- AI supported hearing aids that filter undesired noise and dynamically adopt to the user environment for best performance. Such devices, sometimes also termed wearable devices, may be combined with e.g., fitness tracking, audio streaming or translation functionalities.

Wearables are often equipped with wireless connections (e.g., RFID, NFC, Bluetooth or GSM/LTE) for different purposes, such as transmission or storage of data in smartphones, backend web or cloud applications. This connectivity allows users to access the data almost wherever and whenever desired, or to grant access to stored data and share it with third parties, such as doctors or pharmacists.

3.2 Scope of this study

The examples mentioned illustrate that the definition of a "wearable" encompasses a multitude of different devices. To be considered in this study, devices must be able to measure medical data with sensors and forward the data to another connected device (e.g., smartphone) and/or the internet (e.g., to web or cloud application).



Picture 1: Wearable ecosystem

As this study focused on assessing the security of medical data stored or processed also in the components connected to the wearable device, it did not consider devices operating solely standalone. Standalone devices are fully integrated devices and include data collection and measurement sensors as well as the user interface. However, they do not provide a connection to a mobile or cloud/internet app that could be tested, which is a requirement in this study.

Additionally, the study at hands is targeting wearable devices with the medical functions of pulse measurement and pulse oximetry, at a minimum. While pulse is measured at the finger, arm or chest, the pulse oxygen content measurement takes place at the fingertip, earlobe, or forearm.

3.3 Boundaries

The wearable devices' functionality and the nature of the data collected and processed lead to the assumption that wearable devices as well as the connected mobile and backend applications process highly personal and sensitive data.

In accordance with Article 4 of GDPR Clause 15 and consideration no. 35, literature acknowledges that "health data" comprises all data and information pertaining to the mental or physical health status of individuals, without limitation [12].

In the light of the GDPR, the motivation and title of this study suggest that the data processed by wearable devices, mobile or backend cloud- or web applications must be considered not only as personal data, but also as sensitive health data that requires advanced protection. For wearables covered in this study, advanced protection of health data is seen as a prerequisite for increasing the popularity, acceptance, and use of these devices.

Though GDPR may call for further investigations on privacy and advanced data protection, the focus of the study at hands is set on the technical measures and controls available in the wearable devices and related components for protecting the integrity, confidentiality and availability of the data and information. Neither a detailed analysis of the data protection and privacy guidelines provided by the vendors, nor their implementation, nor the compliance with legal requirements are in the focus of this study.

4 Market analysis

This chapter presents the market situation of wearable devices, and their adoption and usage in Germany. Relevant market segments and device categories are presented, as well as the approach for selecting devices for further analysis.

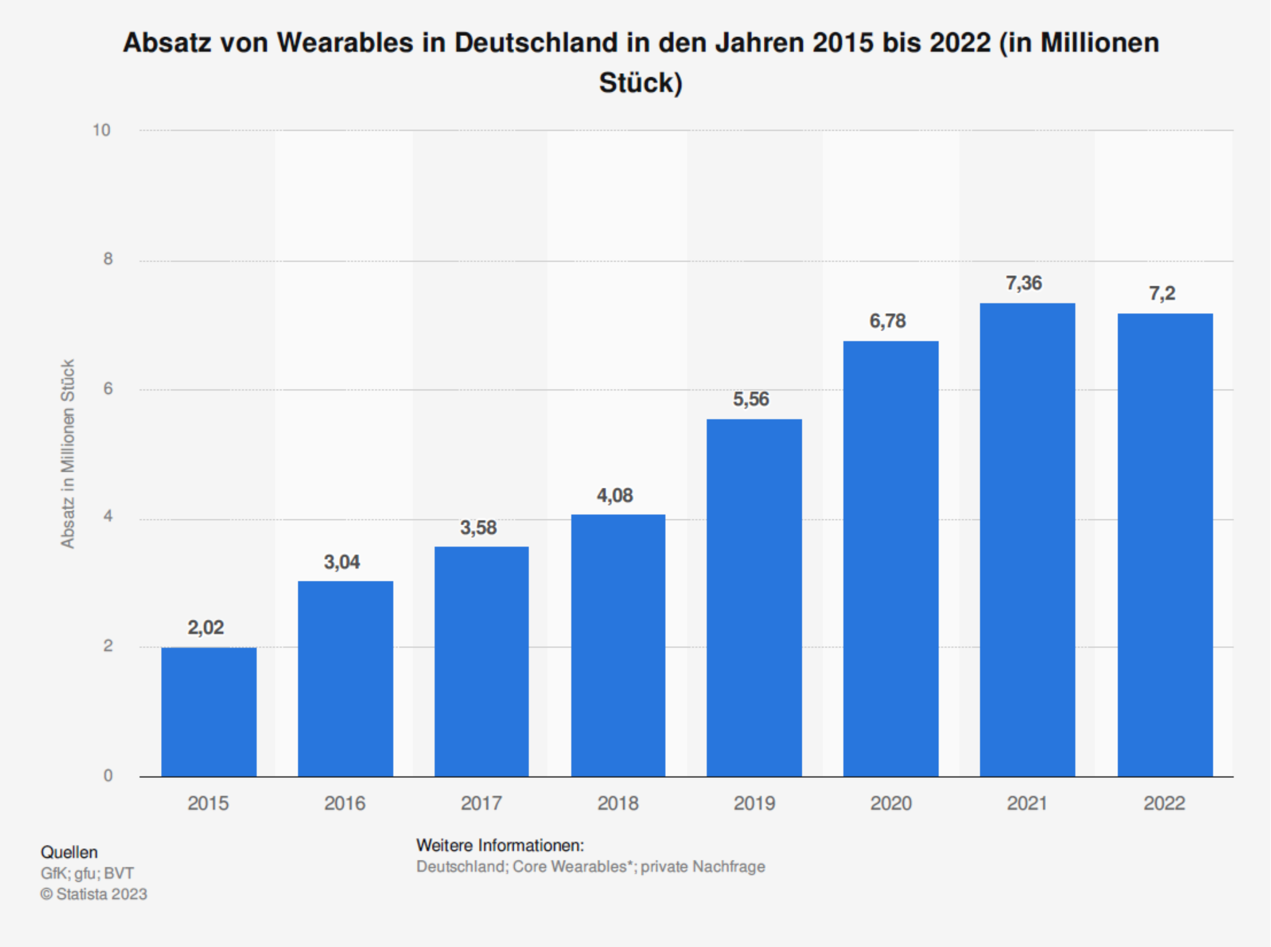
4.1 Market

Wearables are a growing market worldwide and the German market is no exception. The report “Deutschland Wearables Report 2021” ([1]) describes the market development as follows:

> *„The health consciousness of German consumers is the main driver for the growing demand for wearables, which can have a positive impact on both, physical and mental health, in many ways. This in turn creates added value for consumers, especially in the context of the pandemic, which has placed more emphasis on aspects of health. Among others, wearables can help them in better coping with stress and recognizing early signs of an infection".*

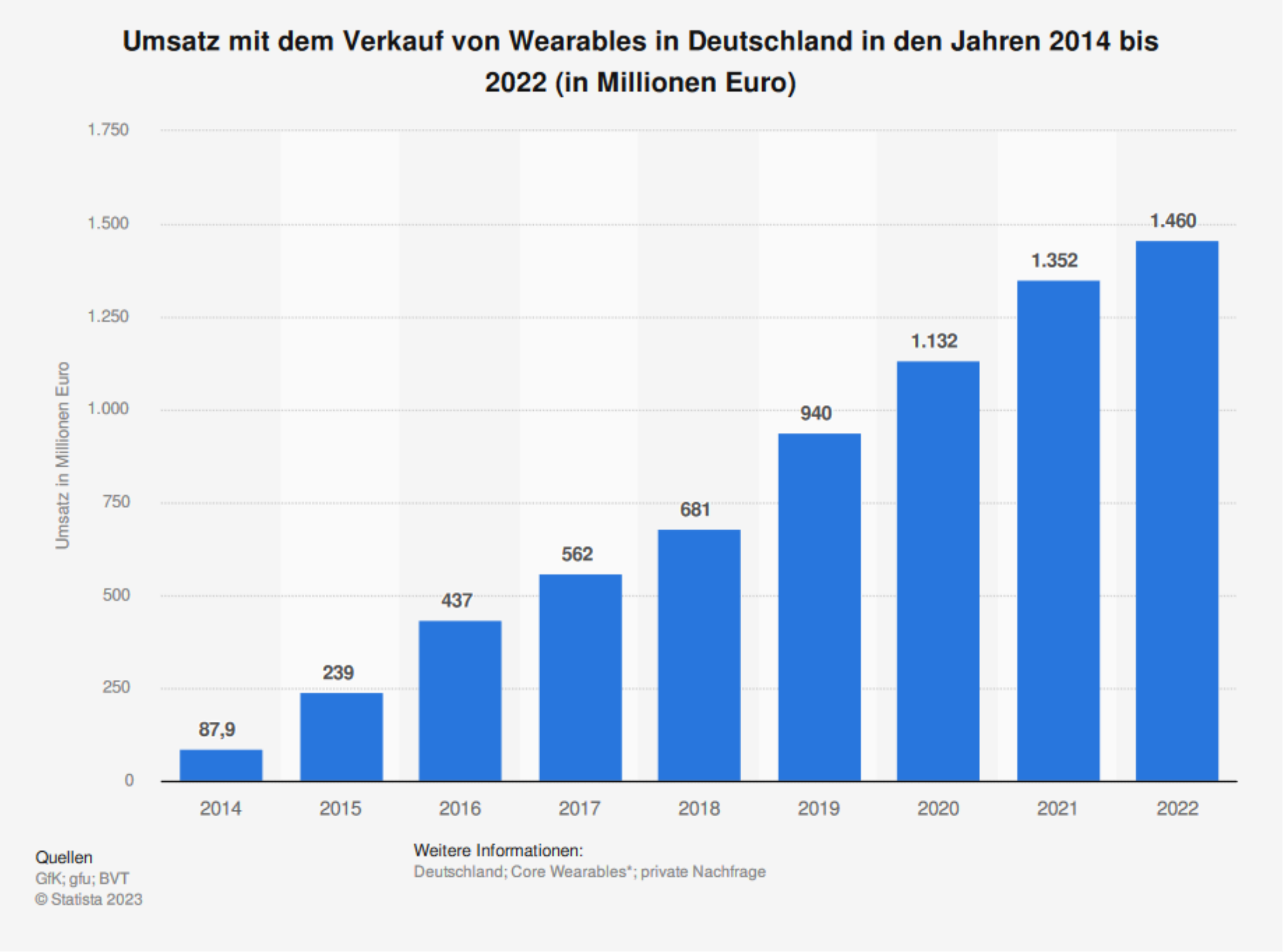
This trend is supported by gfu’s sales and revenue figures regarding the so-called “core wearable” device market segment, including smartwatches (without SIM), smart glasses (without SIM), health & fitness tracker, wrist sport computers, connected watches and tracking devices. [2]

Between 2015 and 2022, sales figures have more than tripled, underpinning the growing relevance and acceptance of wearables devices at consumers. [4]



Picture 2: Sales of wearables in units in Germany, 2015 - 2022

Furthermore, the sales revenue has shown a significant increase, and multiplied by more than six times in the same period from 2015 to 2022. This suggests a trend towards higher-priced devices or devices with a wider range of functions. [5]

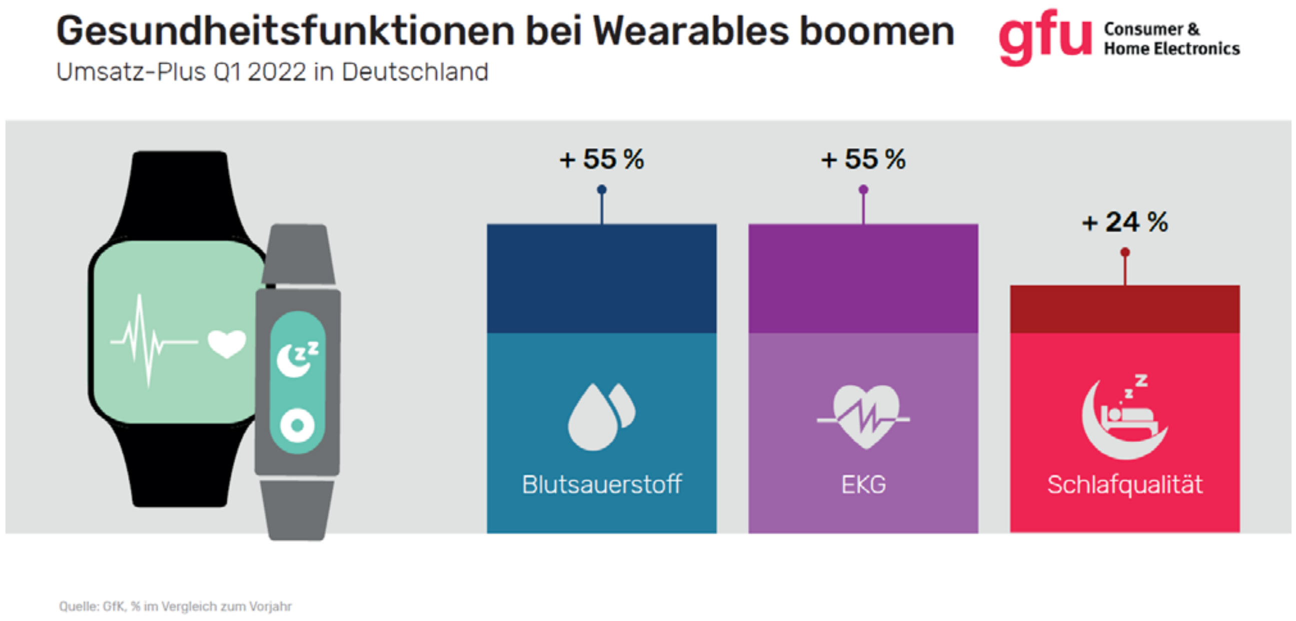


Picture 3: Total revenue of wearables in Germany, 2014 - 2022

A press release of gfu Consumer & Home Electronics GmbH dated 2022 [3] says:

> *"Wearables, smart helpers worn on the body for organisation, communication, sports and health, have enjoyed a steady rise in popularity since their market launch around ten years ago. Double-digit growth rates in turnover and sales are evidence of this year after year. At the moment, when buying wearables, focus is specifically put on health monitoring functions. The little helpers are true multi-talents when it comes to keeping an eye on health data. Wearables that measure heart rate, provide an ECG (electrocardiogram), determine blood oxygen levels or record sleep quality are therefore at the top of the sales with high growth rates.*
>
> *The hit list in terms of growth is led by the function for determining the blood oxygen content: unit sales of these products have almost doubled in 2021 compared to the previous year (+99 percent). And the growth trend continues this year. The first quarter of 2022 saw an increase of 48 percent, compared to last year. In terms of turnover, the growth was even more pronounced: plus 131 percent in 2021 and 55 percent in Q1/2022.*
>
> ***Monitoring ECG, quality of sleep and heart frequency***
>
> *The ECG function is on second place, with unit growth of 89 percent in 2021 and 58 percent in the first quarter of 2022. In terms of sales, devices with this measurement function grew by 64 percent in 2021 and 55 percent in the first three months of 2022. The feature for*

> *monitoring quality of sleep was able to generate an increase of 21 percent last year in units sold, and of six percent during the first quarter of 2022. The growth rate of sales revenue was significantly higher, 58 percent in 2021 and 24 percent in the first quarter of 2022.*
>
> *The heart rate measurement feature using the smart device on the wrist accounted for 10 percent growth of units sold in 2021, and three percent in the first three months of 2022. This led to a 22 percent increase of sales revenue in 2021 and a 19 percent plus in sales revenue in the first quarter of 2022."*



Picture 4: Turnover growth of wearables with medical functions

This supports the trend towards pricier devices or devices with more functionalities to which the growing integration of medical functions into smartwatches contribute.

Additionally, it should be taken into consideration that the average use time of a wearable device varies between five and seven years, see [10]:

Device type	Average duration of use in months (later than 2017)
3.3 Personal telecommunication devices	72
3.4 Mobile phones	72
4.2 Other electronic entertainment devices (UE)	60
7.2 Sports- and leisure devices	84
8.2 Medical products	60

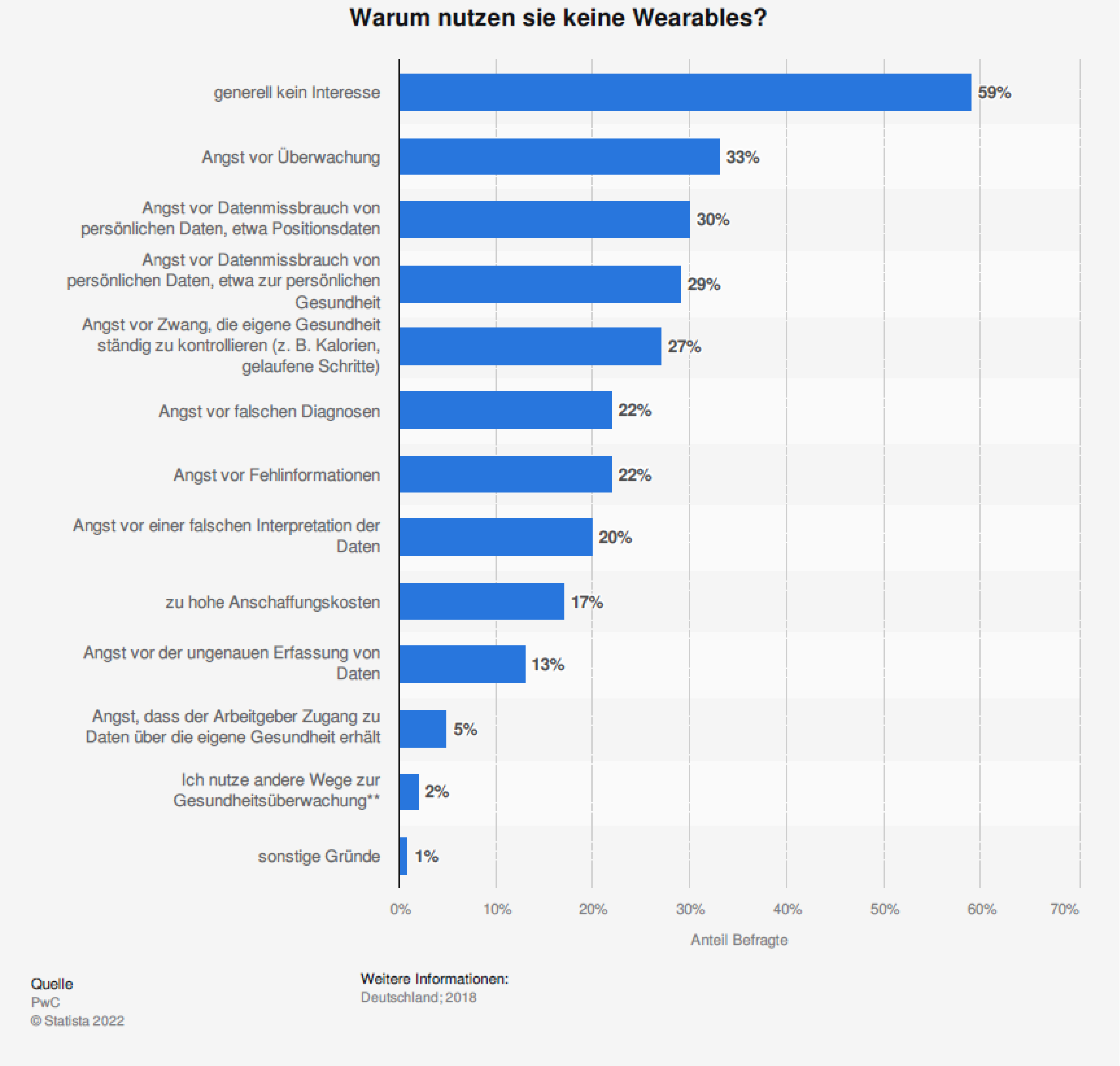
Table 2: Average duration of use

Also, the growing number of users support an increasing relevance of wearables [6]:

> *"In Germany, 29 percent of respondents aged 16 years or older said in 2019 that they at least occasionally privately use a fitness tracker. In 2018, this figure was 26 percent of respondents. In 2019, 36 percent of respondents in Germany aged 16 years or older said that*

> *they at least occasionally use a smartwatch for private purposes. In 2018, this amounted to 28 percent."*

A survey conducted in 2019 looked at the reasons why consumers do not or do not want to use wearables.



Picture 5: Results of a survey in 2018 on reasons not to use wearables

While almost 60% of respondents do to not have any interest in using wearables at all, approximately 30% is concerned about the security of their personal health data, highlighting the importance of protection.

4.2 Device categories

As part of the market analysis, the characteristics of more than 120 wearables devices available in Germany were examined in detail. It was observed that wearable devices are typically positioned in one of the following categories:

- Smartwatches
- Basic watches
- Fitness tracker

- Arm sleeves and chest straps
- Pulse oximeter
- Smart rings.

Since these categories have been established in the market over the time and are widely used, the following sections provide a description of each category.

4.2.1 Smartwatches

Smartwatches used to be watches enhanced with internet connection, primarily used for message transfer, phone calls and data transmission. Nowadays, smartwatches resemble multifunctional mobile computer systems, becoming similar with smartphones regarding their functionality.

Smartwatches are typically sold using the following sales channels:

- e-commerce platforms, such as Amazon, Kaufland or OTTO.de,
- e-commerce shops operated by the developers/vendors,
- specialised retailers (e.g., Intersport, Decathlon),
- wholesale electronic device retailers (e.g., Saturn, MediaMarkt, Medimax),
- retail outlet stores of mobile network operators,
- retailer outlet stores of merchants specialised on watches, or
- memberships in clubs offering access to a proprietary, closed ecosystem.

The market analysis considered approximately 1.1 million smartwatches sold online in Germany in 2022 that have the necessary medical functionalities.

4.2.2 Basic watches

Basic watches are a specific sub-segment in the segment of smartwatches, aiming at price-sensitive consumers. Basic watches are positioned between (simplistic) wristbands and multi-functional smartwatches. Typical characteristics are:

- small displays, reduced and limited functionalities and low battery capacity;
- rudimentary operating system;
- lack of support for third-party apps.

The category of basic watches corresponds to the segment of smartwatches at a price of less than 100 EUR.

4.2.3 Fitness tracker

Fitness tracker devices originated in the realms of sports and fitness. Vendors have continuously incorporated additional features into trackers, making it increasingly challenging to differentiate between trackers, basic watches, and smartwatches. This distinction is now frequently utilised by vendors to intentionally position devices within a particular target market segment.

The survey analysed around 267,000 fitness trackers that were sold through e-commerce platforms in Germany during 2022. These trackers had minimum required functionalities for measuring pulse and pulse oxygen content. It shall be noted that many devices in the fitness tracker segment do not provide for the required medical functionalities. It is remarkable that the market share of no name products in the fitness tracker market segment is about 14%, which is significantly less than in the segment of smart watches.

4.2.4 Arm sleeves, chest straps and pulse oximeters

Arm sleeves, chest straps and pulse oximeters are commonly used in the medical domain and in sports. These devices often provide more reliable measurement results for pulse and oxygen content in the blood in comparison with measurements performed at the wrist. For measurement of pulse, arm sleeves and chest straps provide better results than a smartwatch positioned at the wrist. Therefore, these devices are often used in sports as an extension of or in addition to a smartwatch or smartphone and use wireless connection.

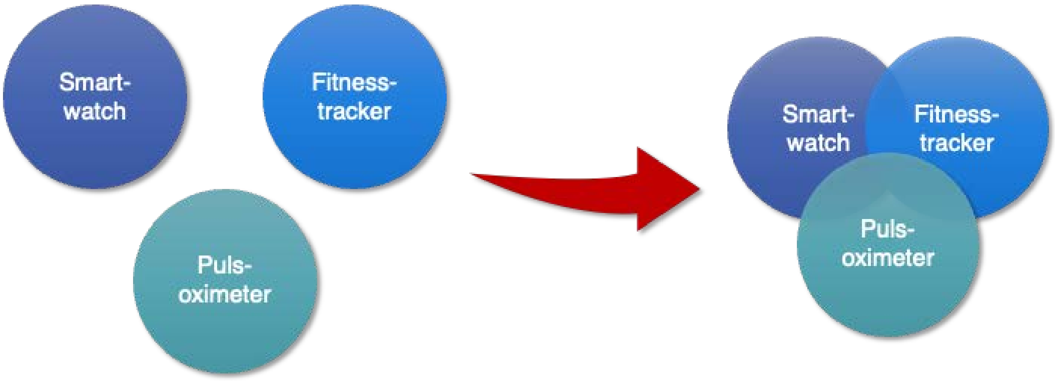
Pulse oximeters are rooted in the domain of medical devices. Most of them are operate standalone, i.e., sensors and user interface (e.g. display or function keys) are integrated in a single device without any connection to a peripheral device. Except from sports in greater altitudes or during flights, use of such devices is typically medically indicated. These devices are usually sold at pharmacies or medical supply stores on prescription or advise of a doctor.

4.2.5 Smart rings

Smart rings are relatively new in the market and worn on the finger. Smart rings are an approach to realise a wearable device with a discreet form factor. It remains unclear at present whether these devices will achieve widespread popularity and capture a significant market share, given the multitude of smartphones that offer comparable or even greater functionality. Unfortunately, no relevant data or statistics regarding the smart ring market segment in Germany were obtainable.

4.2.6 Boundaries

While in the past, wearables in the categories smartwatch, fitness tracker or pulse oximeter were easily distinguishable from each other, these categories are today less sharply separated. Boundaries have become blurred because of the increased integration of functionalities into devices.



Picture 6: Overlapping categories

Although the categories smartwatch and fitness tracker are not precisely distinguishable, they represent the two largest and most significant market segments. To consider them separately, the differentiation or categorization of devices was based on the manufacturer's advertising statements and positioning.

4.3 Selection of wearables

To obtain an overview of the devices relevant in the aforementioned categories, the following approach was followed:

- review of publications for identification of the market-leaders;
- identification of the devices relevant for the market overview by means of research on manufacturers' websites;

- researching e-commerce platform “amazon.de” about sales volumes and market prices in 2022 and April 2023;
- identification of other devices relevant in the market segments of interest, not manufactured by one of the market leaders. This was achieved by review and analysis of ranking lists at “amazon.de”;
- determination of manufacturers' market shares (> 0.3%);
- listing of devices for each category in scope;
- gathering of the technical details per device as available on manufacturer and retailer websites.

To avoid influencing and distorting the results of the market survey due to varying levels of cooperation, manufacturers were not approached. As a result, the sales and turnover statistics do not include manufacturer information.

For the research of sales volumes of the devices in Germany meeting the previously mentioned criteria, analysis tools for the leading online retail platform "amazon.de" were used.

In 2021, the website and marketplace “amazon.de“ accounted for almost 50% of e-commerce sales revenue of the ten largest B2C online shops in Germany, which together account for more than 41% of sales in the total market. Market share of “amazon.de” in B2C e-commerce sales in Germany for 2021 was almost 20%. At the same time, “amazon.de” is the leading marketplace in Germany, generating approximately 61% of the gross trade volume of a list of ten selected pure or hybrid marketplaces in 2021. Of the 1000 leading online shops, a substantial proportion also sell their goods via marketplaces; 43% of all e-commerce retailers do additionally have a profile on Amazon [11].

Furthermore, as consumers have a clear preference for buying electronic goods online over buying them in brick-and-mortar retail outlets (45 % online vs. 19 % brick-and-mortar outlet stores, see [7]), the information available is considered as suitable and relevant for identification of manufacturers.

Among the categories of wearables listed in the preceding section, pulse is measured on the finger, arm or chest, while blood oxygen content is measured on the finger, earlobe (only in medical cases) or forearm.

Based on the results of the market analysis and taking the project objectives of targeting devices that provide at least for the two medical functionalities pulse and blood oxygen content measurements into account, the further detailed analysis was limited to the following four categories

- smartwatches
- basic watches
- fitness tracker and
- smart rings.

Next, devices in each of the four categories were selected using the criteria “sales figure” and “actuality of product” as follows:

- Sales figure: the sales figure, i.e. number of devices/units sold, were determined based on the results of the market analysis and analysis of sales figures available for the e-commerce platform “amazon.de”. To improve the quality of results, sales figures of wearables of a product series were summed up.
- Actuality of product: to avoid assessing wearables carrying vulnerabilities that have already been remediated in a later product of the same product series, only the latest device of a series was selected.

Smart rings form a new market segment. Within this market analysis, it was not possible to determine reliable sales figures. Additionally, the majority of products was not available for purchase or has only been announced so far. Since the market share of smart rings is believed to be low and the evaluation criteria could not be applied, one product was selected as a representative sample for this category.

The available budget allowed to select 10 wearable devices for further analysis, among which were:

- Three smartwatches,
- Three basic watches,
- Three fitness trackers and
- One smart ring.

Whenever possible, the cheapest variant of a device in a product series with variants (e.g. wrist bands in plastics, leather or steel, colour black or coloured, different device sizes for women and men) was finally purchased for further analysis.

The devices were purchased between 22 June and 30 August 2023.

5 Cybersecurity review

The main objective of the SiWamed project and the cybersecurity review was the identification of vulnerabilities in wearable devices, connected mobile apps and backend systems. With the assessment, the testers analysed the security of the software implementation and tried to gain unauthorised access to the devices, its functionalities and data processed.

This chapter commences with a description of the security testing procedures applied throughout the assessment in Section 5.1.

The rating of vulnerabilities in the assessment and this report is introduced in Section 5.2.

In the absence of a security testing standard applicable to wearables and their components, the project team developed a bespoke test plan. The test plan was derived from existing recognized related standards and best practices, and took the expertise and experiences of the penetration testers into account. A high-level summary of the test plan is presented in Section 5.3.

To ensure a comparability of results, the test plan was applied identically to each wearable, resulting in a detailed, non-publicly available penetration test report per wearable. BSI shared these reports with wearable vendors using a coordinated vulnerability disclosure procedure.

The summary of the security assessment results is presented in Section 5.4, augmented by a description of selected vulnerabilities.

In Section 5.5 this chapter concludes with some observations and impressions gained by the testers throughout the assessment.

5.1 Security testing procedures

This section introduces the tests and procedures that were applied for assessing the security of a wearable, consisting of the wearable device, the mobile app and the backend.

For the sake of clarity, the terms “wearable” and “wearable device” are used in the remainder of this document with distinct meanings. A “wearable” has a broader meaning and comprises the wearable device including the sensors, as well as the device vendor’s related components mobile app and backend. The wearable device refers to the core unit with integrated sensors that is worn on the body.

The testers conducted the assessment of each wearable in a period of four days, which included the development of a detailed penetration test report. Emphasis was placed on assessment of the wearable device. However, since the device is usually connected to a mobile app and a backend, and shares data with, both components were additionally considered in the scope of the assessment.

The project’s constraints in terms of time and budget, and the legal obligations necessitated the exclusion of some tests, such as

- Hardware-related tests, including
  - Physical tests, to test resilience of the device against e.g., opening and tampering, accessing JTAG debug ports (if available), or electro-magnetic fault injection;
  - Logical tests to test the resilience of the device against e.g., side channel analysis on cryptographic functions, fuzzing of interfaces;
- Tests related to the implementation of WIFI, NFC and Bluetooth protocol stacks;
- Tests related to implementation of GSM or LTE protocol stacks;
- Detailed analysis and reverse engineering of the device’s firmware;
- Detailed tests on the backend infrastructure;

- Analysis of privacy policies.

5.1.1 Wearable device

The security testing procedures applicable to wearable devices were customised to the device's characteristics and interfaces. The tests for the devices covered at least the following modules, components and interfaces:

- Operating system
- Apps
- Bluetooth
- USB
- WIFI

In detail, the following tests were performed:

Interface/ Component	Test item
Operating system	Tests for missing security updates
	Tests regarding hardening
	Tests to access the configuration of OS or apps that should not be accessible to users
USB	Tests regarding availability and accessibility of test interfaces (e.g. ADB)
	Tests regarding the ability to sideload and install apps using the debug interface
	Tests regarding the ability to download new apps
	Tests regarding the ability to read data stored on the device
	Tests regarding other functionalities supported by the debug interface (e.g. debugging, logging)
Bluetooth	Tests regarding the version used
	Tests regarding the pairing mechanisms supported (legacy, SSP)
	Tests regarding resilience against Machine-in-the-Middle attacks, depending on the pairing method used
WIFI	Tests regarding the services offered via WIFI interface (e.g., ADB over wireless, local web server, telnet etc.)
	Tests regarding Machine-in-the-Middle attacks (e.g., encryption, certificate validation and certificate pinning)

Table 3: Wearable device test items

5.1.2 Mobile app

The test selected for assessing the security of the mobile apps are derived from the globally recognized and widely acknowledged standards

- OWASP Mobile Application Security Verification Standard (MASVS) [13] and
- OWASP Mobile Application Security Testing Guide (MASTG) [14].

The tests conducted can be separated in two categories:

- Tests regarding the quality of mobile app implementation test if, which and at which quality measures have been implemented to protect sensitive data. A missing or incorrectly implemented security function was considered as a vulnerability, even it did not necessarily have to be exploitable. These tests were derived from OWASP MASTG Level 1 and Level 2 tests, testing the availability and correct implementation of protections and use of security services of the platform. The tests assumed that the platform was trustworthy, i.e., the mobile app relied on the integrity of the platform and the security services provided.
- Tests regarding the resilience of the mobile app check which protections have been implemented to protect the mobile app against advanced attackers using reverse engineering and tampering techniques. Protection mechanisms are e.g., emulation detection, root detection, hooking detection, obfuscation, or device binding. These tests were derived from OWASP MASTG Level -R(esilience) test catalogue and based on the assumption that the platform was actually compromised so that the mobile app could security-wise no longer rely on the platform services. The resilience tests were distinct from Level 1 and 2 tests, and they constituted an additional set of tests. The tests applied in this study focused on the availability of protections in the mobile app against advanced attackers, but not on the assessment of their resilience.

The tests performed were targeting following features:

- Authentication
- Secure data storage
- Usage of platform security features
- Secure network communication
- Rooting detection
- Hooking detection.

5.1.3 Backend systems

Backend systems are typically composed of

- web and cloud applications and APIs,
- operating systems and cloud services/components, and
- active network components and other active appliances.

Within this project, no attempt was made to obtain the consent of the manufacturers to carry out detailed or advanced tests of the backend systems. In such cases, the legal framework necessitates a limitation and restriction of the scope and the depth of tests. Accordingly, tests targeting the operating systems, cloud services/components and other infrastructure systems were generally excluded.

Tests targeting web applications and APIs were limited to the following categories:

- Client-side controls
- User authentication

- Session management
- Access control
- Injection
- Logical errors
- Information disclosure: logging, error messages

5.2 Rating of vulnerabilities

For better comparability of results, each vulnerability identified during the tests was assigned a score using the CVSS methodology, see [15] for details. Vulnerabilities were grouped according to their severity applying the CVSS v2 score as follows:

Severity	CVSS v2 score	Description
Critical	10.0	Vulnerabilities that need to be addressed immediately. For example: the vulnerability leads to full take over the affected system, it is exploitable over the network and a public "one-click" exploit is available.
High	7.0 - 9.9	Vulnerabilities that need to be addressed in the short term.
Medium	4.0 - 6.9	Vulnerabilities that should be addressed during the next regular maintenance schedule.
Low	1.0 - 3.9	Vulnerabilities rated as low are usually potential configuration improvements and/or difficult to exploit. These should be addressed during an internal risk management process.
Informational[1]	0.0 - 0.9	These are mostly not vulnerabilities by themselves. For example, information gathered during the penetration test, such as open ports and software versions. There is no need to address these items.

Table 4: CVSS v2 vulnerability rating

It shall be noted that the comparison of ratings in different wearable components has limitations. E.g., a vulnerability on a device requiring physical access may lead to the compromise of the data and information of one individual person per attack. A vulnerability in the backend with a similar rating may allow an attacker to gain access to information belonging to millions of people. The ratings do not anticipate the risks associated with consequences of an exploitation.

5.3 Test results

As mentioned in section 4.3 above, ten wearables were selected for further analysis, among which were

- three smartwatches,
- three basic watches,
- three fitness trackers and
- one smart ring.

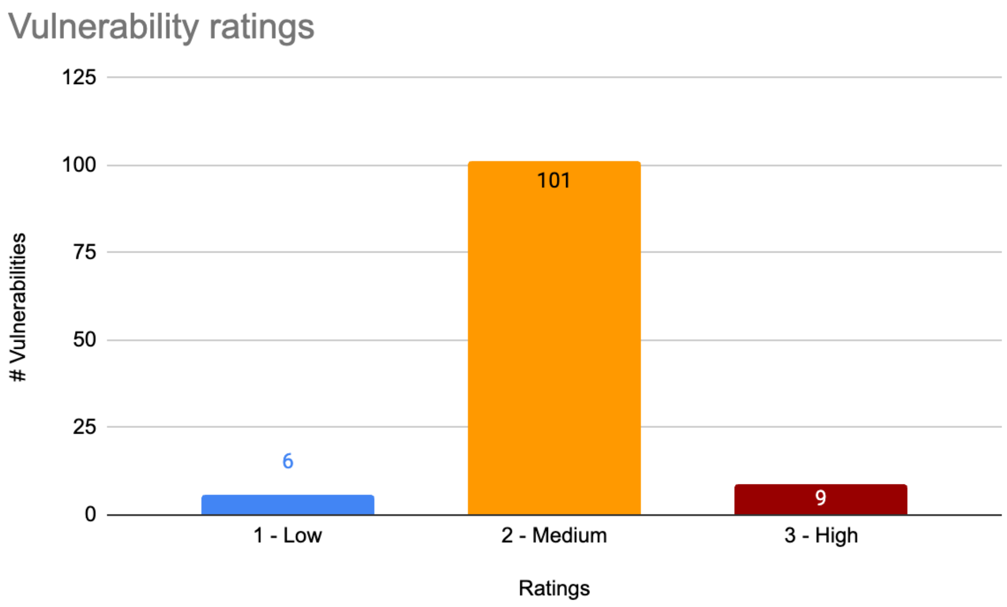
[1] The testers identified altogether twelve vulnerabilities rated "Informational". In the remainder of this report, however, these weaknesses will not be further considered.

In summary, during the assessments a total of 34 unique vulnerabilities with 116 occurrences across the wearables and their components were identified.

113 vulnerabilities were confirmed, three vulnerabilities were considered potential which means that the testers experienced major inconsistencies when reproducing the vulnerabilities, e.g. due to possible software changes, updates or general instability of exploit proof of concept (POC). Note that both types of vulnerabilities, confirmed and potential, were retained in the further analyses.

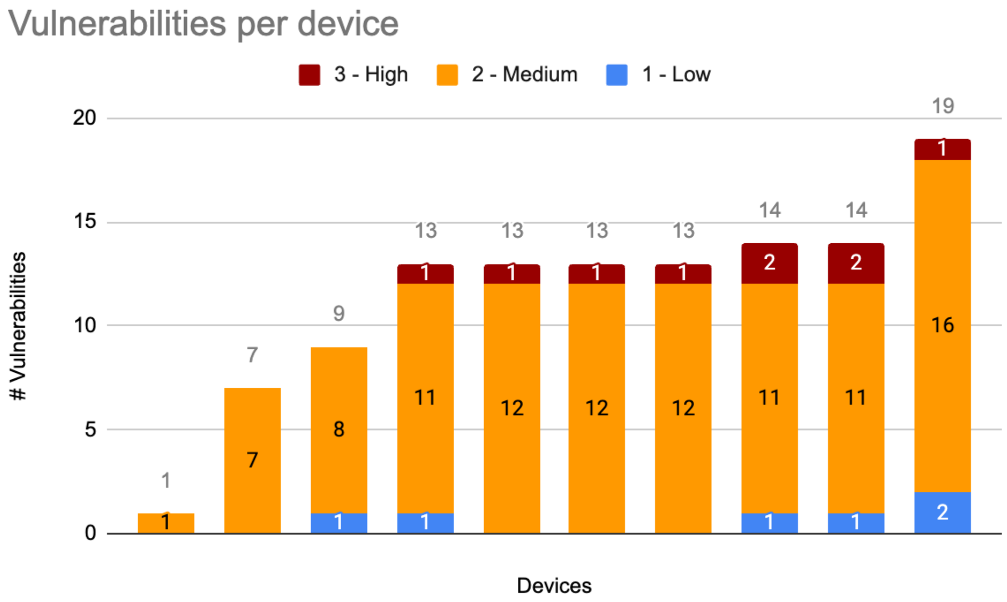
Six vulnerabilities rated “Low” in five different wearables were identified, either in the device, in the mobile app or in the backend. Nine vulnerabilities found on seven wearables received the rating “High”, while the majority of vulnerabilities (101 of 116) identified in the course of the assessments were rated “Medium”.

Vulnerabilities rated “Critical”, which would have called for immediate action, could not be identified.



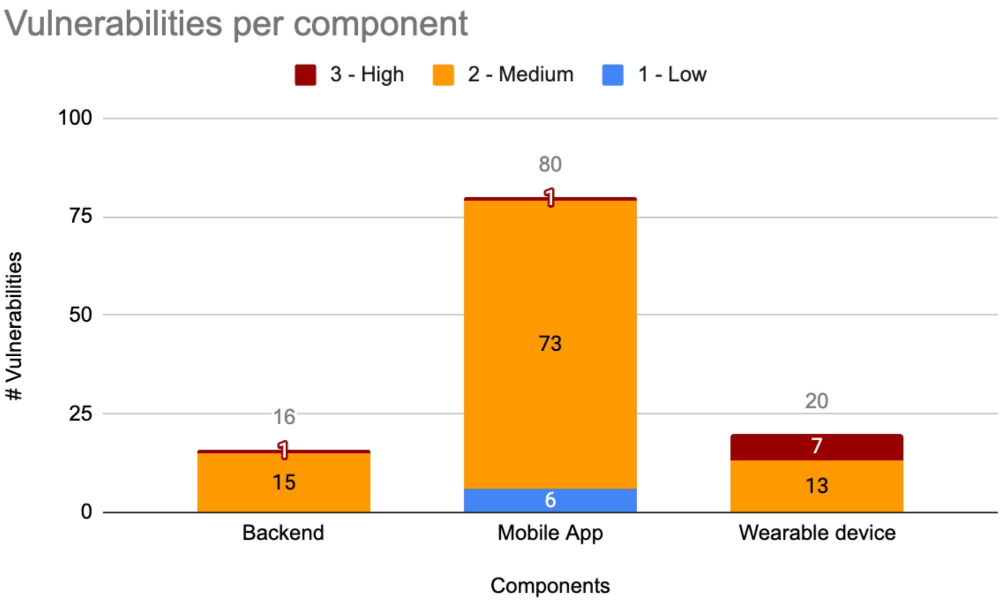
Picture 7: Rating of vulnerabilities

Notably, none of the wearables was found to be free of any vulnerabilities. Seven wearables carrying one or more vulnerabilities rated “High” additionally suffered from at least eleven “Medium” rated vulnerabilities, as shown in the following graphics.



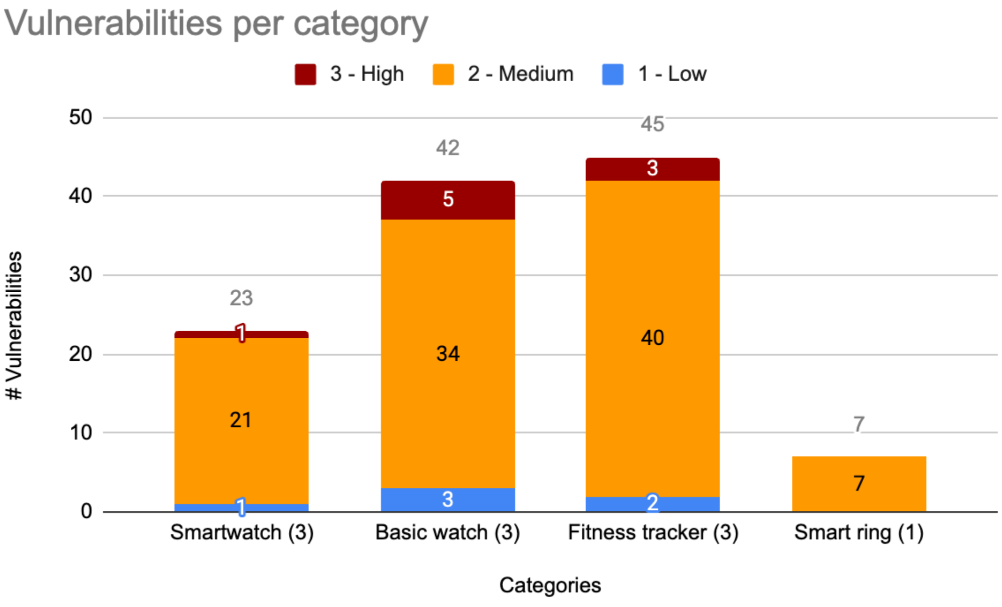
Picture 8: Vulnerabilities per device

Further analysis of the vulnerabilities uncovered that most (seven of nine) vulnerabilities rated "High" were located in the wearables devices, one in a mobile app and one in a backend. Though, the majority of vulnerabilities rated "Medium" were located in the mobile app.



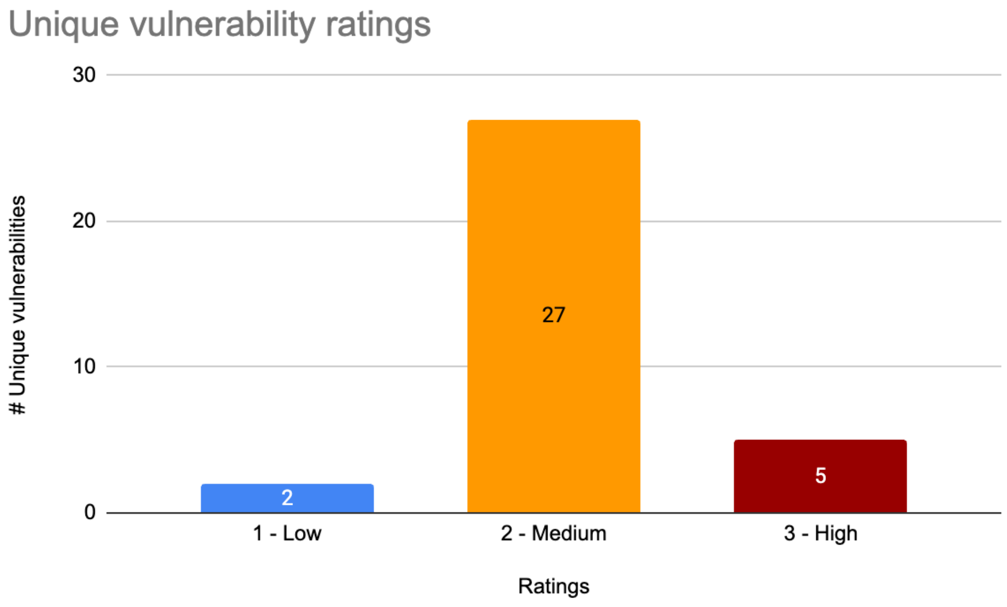
Picture 9: Vulnerabilities per component

The following chart displays how the 116 identified vulnerabilities are spread over the wearable categories "Smartwatch", "Basic watch", "Fitness tracker" and "Smart ring". Here, it shall be recalled that the assessment included three devices of each of the first-mentioned categories, and one Smart ring.



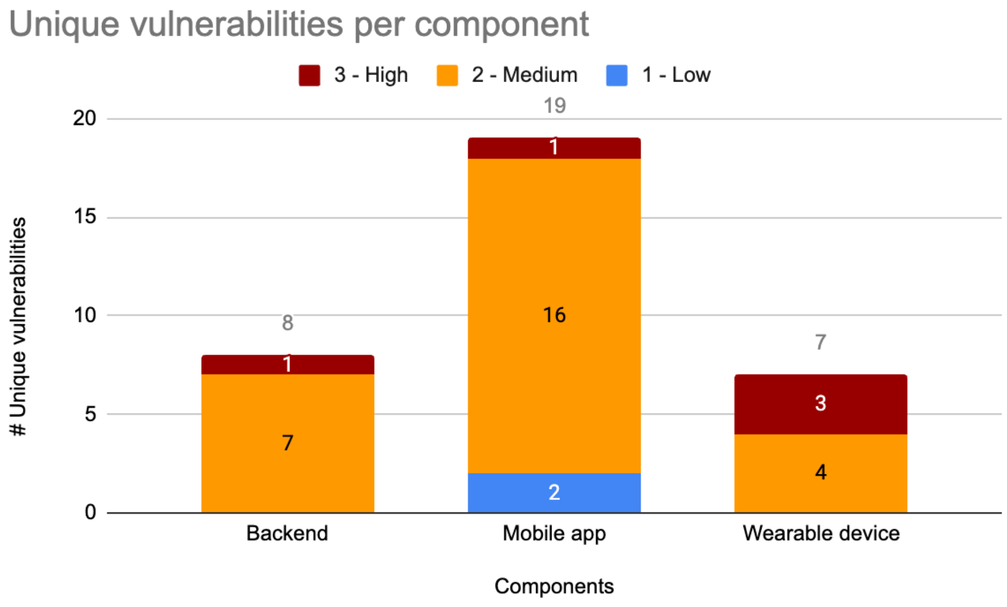
Picture 10: Vulnerabilities per category

During the assessment, the testers identified 34 unique vulnerabilities across the total set of 116. Five unique vulnerabilities are rated “High”, 27 “Medium” and 2 “Low”, as shown below. Note that a unique vulnerability designates a vulnerability that is observable in one or multiple wearables.



Picture 11: Rating of unique vulnerabilities

The following charts shows how the 34 unique vulnerabilities distribute over the wearable components.



Picture 12: Unique vulnerabilities per component

A list of all 34 unique vulnerabilities identified during the assessment is contained in Appendix A, together with their CVSS score, rating and frequency of occurrence.

5.4 Description of selected unique vulnerabilities

In this section, all five unique vulnerabilities rated “High” as well as the unique vulnerabilities found most often in a wearable component are described. Together, both sets represent 78 of all 116 vulnerabilities observed during the assessment.

5.4.1 Vulnerabilities rated “High”

The following table lists the vulnerabilities rated “High”, the component affected as well as the frequency of occurrence. Below, the vulnerabilities are described in more detail.

Vulnerability	Rating	Component	Occurrences
Account takeover via HMAC secret bruteforce, see 5.4.1.1	8.5	Backend	1
Pairing PIN bypass, see 5.4.1.2	8.3	Wearable device	3
Bluetooth MITM, see 5.4.1.3	8.0	Wearable device	2
Bluetooth pairing without confirmation, see 5.4.1.4	7.6	Wearable device	2
Insecure Android SSL library, see 5.4.1.5	7.4	Mobile app	1

Table 5: Vulnerabilities rated "High"

5.4.1.1 Account takeover by HMAC secret bruteforce

The JSON Web Token specification provides several ways for developers to digitally sign payload claims which ensures data integrity and robust user authentication. Whenever developers use HMAC signatures, they need to provide a secret key, which is used for both signing and verifying tokens. If this secret is cryptographically not strong, the whole signature can be compromised. If the secret can be brute-forced this way, a malicious user can modify the JWT header and payload, then resign the token with a valid signature for the server. After that they can use this token to access a user API and take over the victim user account.

5.4.1.2 Pairing PIN bypass

If there is physical interaction in Bluetooth pairing sequence it sometimes can be bypassed e.g. by sending special requests or recording/repeating successful pairing.

In this case device pairing sequence was including the PIN that the user needs to enter into the mobile application to pair the device. During the tests a way to bypass the PIN protection with specially formed requests was found. Because it was possible to connect multiple devices and multiple accounts without manually wiping the device the outcome in case of an attack is similar to the "Bluetooth pairing without confirmation" vulnerability, see 5.4.1.4.

5.4.1.3 Bluetooth MITM

During the attack, one of the Bluetooth adapters was used to connect to the target wearable. Subsequently, a second adapter was used to advertise the Bluetooth connection instead of the original wearable. During any exchange the data that comes from one connection is re-directed through the software proxy into the connection to the other Bluetooth adapter. When such an attack is performed the victim user connects to an attacker-controlled device instead of a wearable. Then any Bluetooth communication performed can be recorded, tampered and repeated. In case the data is transferred in unencrypted form, the attacker has full control of sensor data, SMS, account data, installed apps/firmware update files etc. To protect from attacks of this class, it is important to encrypt the data transferred and implement multi-stage Bluetooth pairing handshakes and drop the connection if handshake requirements have not been met.

5.4.1.4 Bluetooth pairing without confirmation

Design and implementation of a secure pairing sequence is challenging. Pairing a device requires not only following a particular protocol, but also a specific sequence of actions to connect a wearable device. If there is no direct physical interaction with the wearable during Bluetooth pairing it means the attacker can try to connect to the victim wearable that is in general proximity - it can be done for example in public spaces. Another key consideration is whether it is possible to connect multiple mobile applications to the same wearable and whether you need to wipe data before you connect or not. Pairing sequence attacks become less viable if it is not possible to connect to multiple accounts. In view of this, the most straightforward method of securing a pairing sequence is to require the wearable to be wiped before pairing again. If there is a means of connecting an additional device, it also opens up the potential for an "evil maid attack," in which an assailant targets an unattended device. If connecting another mobile application is necessary, it is recommended that you implement a device PIN and require it every time a device is paired. Wearables without a direct physical interface should not permit multiple pairing.

5.4.1.5 Insecure Android SSL library

The usage of the Android API SSLSocketFactory is prone to Man-in-the-Middle attacks because it does not verify the certificate hostname. Trusting any certificate or accepting self-signed certificates is a critical security issue. The application is vulnerable to Man-in-the-Middle attacks and transiting sensitive data can be intercepted, exfiltrated and/or tampered with. This may also change the behaviour of the application and/or the backend server.

5.4.2 Most frequent unique vulnerabilities in components

The below table lists 13 of 34 unique vulnerabilities, which were found 72 times and account for more than 60% of all observed vulnerabilities. They were the most frequent vulnerabilities in each component and represented at least 50% of all identified vulnerabilities per component.

Vulnerability	Rating	Component	Occurrences
Vulnerable JavaScript dependency, see 5.4.2.1	4.2	Backend	5
Cross-origin resource sharing: arbitrary origin trusted, see 5.4.2.2	6.3	Backend	3
Unencrypted communication, see 5.4.2.3	4.3	Backend	3
Critical permission(s), see 5.4.2.4	6.4	Mobile app	9
Repackaging - setting debuggable flag, see 5.4.2.5	6.3	Mobile app	9
Insufficient root detection, see 5.4.2.6	4.6	Mobile app	9
Insufficient hooking detection, see 5.4.2.7	4.6	Mobile app	9
Insufficient SSL pinning implementation, see 5.4.2.8	4.3	Mobile app	9
User authentication missing on device, see 5.4.2.9	6.6	Wearable device	4
Pairing PIN bypass, see 5.4.1.2	8.3	Wearable device	3

Vulnerability	Rating	Component	Occurrences
Pairing to multiple accounts, see 5.4.1.4	6.9	Wearable device	3
Arbitrary application installation, see 5.4.2.10	6.9	Wearable device	3
User authentication insufficient on device, see 5.4.2.11	6.6	Wearable device	3

Table 6: Most frequent unique vulnerabilities in components

In the following, these vulnerabilities are described in more detail.

5.4.2.1 Vulnerable JavaScript dependency

The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS. During the penetration test some outdated and non-maintained JavaScript libraries were identified (e.g. jquery, moment.js) with known vulnerabilities. During this assessment, it was not verified if the vulnerable functions of these third-party libraries are actually used and therefore exploitable. Nevertheless, the patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in the application should be improved.

5.4.2.2 Cross-origin resource sharing: arbitrary origin trusted

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request. Trusting arbitrary origins effectively disables the same-origin policy, allowing two-way interaction by third-party web sites. Unless the response consists only of unprotected public content, this policy is likely to present a security risk. If the site specifies the header Access-Control-Allow-Credentials: true, third-party sites may be able to carry out privileged actions and retrieve sensitive information. Even if it does not, attackers may be able to bypass any IP-based access controls by proxying through users' browsers.

5.4.2.3 Unencrypted communication

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer.

5.4.2.4 Critical permission(s)

Most of the wearables operate with critical Android data and resources, such as SMS, phonebook or Android account information, and perform administrative actions for wearables - such as downloading and installing updates, pairing and disconnecting wearable via Bluetooth. In many cases, the permission list that an application requests includes dangerous permissions that could be avoided.

5.4.2.5 Repackaging - setting debuggable flag

Attaching a debugger to an application is one way for an attacker to dynamically analyse an application. Using this dynamic analysis an attacker can:

- Modify the application execution and bypass any client-side checks.
- Inspect any data at any moment of the application execution. This can be used to log critical data once it has been decrypted.
- Analyse the application more efficiently to break the intellectual property of the developers.

5.4.2.6 Insufficient root detection

Most of the mobile applications do not have any root detection or use only basic ways to detect a rooted device. Applications that handle critical data should not allow running on rooted devices both for user safety and as an anti-debugging measure.

Having root access or running a mobile app on a rooted device actually removes all core security functions of the Android platform, such as isolation of mobile apps, provision of secure communication channels, and many others. Gaining full control over their devices may be a desirable objective for a few mobile device users. However, taking full control over a device is one of the main objectives for malware and attackers, as being a “root” user grants the attacker full and unlimited access to all information and components on the device.

Because a mobile app cannot distinguish between a legitimate friendly “root” user and an adversarial “root” user on the device, sensitive apps should check whether a device is rooted or not. If the result is positive, then it is reasonable to assume the mobile device as compromised and consider the platform untrustworthy. This shifts the responsibility for detecting a rooted device to the mobile app or, to put it correctly, to the mobile app developer. It can be only his duty to manage the risks of running on a rooted device.

5.4.2.7 Insufficient hooking detection

Many mobile applications do not provide for hooking detection or use only basic ways to detect hooking attacks. Applications that handle critical data should detect hooking attempts both for user safety and as an anti-debugging measure.

Hooking is currently the most used technique to perform dynamic analysis and instrumentation of an Android or iOS application. In the last few years, FRIDA has become the most used hooking framework. Its ease of use, and great extendibility, makes it usable by both beginner and expert attackers. It is particularly useful for advanced reverse engineering or for implementing attacks. Using this dynamic analysis, an attacker can::

- Modify the application execution and bypass any client-side checks.
- Inspect any data at any moment of the application execution. This can be used to log critical data once it has been decrypted.
- Analyse the application more efficiently to break the intellectual property of the developers.
- Disable root detection.

5.4.2.8 Insufficient SSL pinning implementation

Most of the mobile applications do not have SSL pinning implemented. That allows attackers to easily inspect the traffic between their mobile application and remote servers by installing certificates.

Due to inadequate implementation of SSL pinning, it was possible to execute a Man-in-the-Middle (MITM) attack and intercept traffic between the mobile application and remote service. An attacker can leverage this information to observe and modify the application flow by repeatedly altering the requests sent by the application, thus effectively crafting attacks. In combination with protections against hooking and repackaging, SSL pinning presents an efficient method for hardening mobile applications.

5.4.2.9 User authentication missing on device

The wearable is not protected by any authentication mechanism. In case of a lost or stolen device all information stored on the wearable can be accessed without any authentication.

5.4.2.10 Arbitrary application installation

Wearable devices differ heavily in their capabilities, but a lot of them are offering watch face installation and some allow application installation. On the other hand, an attacker after finding initial vulnerability needs to find a way to use it to expand the attack. The vulnerabilities in the application/watch face installation process can allow an attacker to install on the wearable a malicious application that may harvest and send sensor data. For this to be possible the device should initially support application installation and execution of scripts. Watch faces often come in the form of archives with images, JSON data and sometimes JavaScript files, though JavaScript execution is reduced to a small list of functions usually. Installable third-party applications on the other hand often have more powerful capabilities and, in some cases, can even send http requests to remote targets. If an attacker manages to leverage their initial access to a device to install harmful applications, the risks rise significantly. To mitigate this the applications installed should be monitored and user-provided applications, non-signed applications should be allowed to be installed only with developer mode on. Ideally every installed application should have a signature that can be checked on the wearable locally.

5.4.2.11 User authentication insufficient on device

The wearable is not protected by any authentication mechanism by default. The PIN is implemented, but it is only requested for special functions like payments and not for accessing health data. Additionally, some devices were asking for the PIN to reset the device, but the health data was not affected by the reset.

5.5 Other observations

The most common vulnerabilities found in wearable devices are related to user authentication and Bluetooth communication. Many devices are lacking any sort of user authentication, using e.g. a PIN, or provide a vulnerable implementation.

Seven of the eight vulnerabilities rated “High” were related to the Bluetooth protocol which serves as the main channel to connect the wearable device to the mobile app.

It shall be highlighted that attacks on wearable devices usually have limitations - for most of them, the attacker needs to be in the Bluetooth proximity, same WIFI network or have physical access to the device.

Most of the tested mobile apps do not provide basic anti-debug protection or rooting/hooking detection. These protections would help to increase the mobile app resiliency, better defend against advanced attackers and protect the user data against attacks on the platform or the app.

Because most mobile apps neither implement certificate pinning nor properly establish a Bluetooth communication channel, it was possible to eavesdrop the firmware during the update process. The firmware could have then been analysed and tampered with by an attacker if not properly protected, e.g. by signatures or checks for information leaks.

Note that a detailed analysis of the wearable firmware for vulnerabilities or any other unwanted behaviour was beyond the scope of this project. Also, the recorded Bluetooth traffic was analysed only on a basic level during this project. Without further analysis, it was not possible to determine if these issues are supportive for exploitation of a vulnerability, e.g. in the firmware.

The testers observed that some vulnerabilities were recurring because of use of unified device operation systems, software and use of shared infrastructure. This raised concerns because of the risk of large-scale attacks on many devices at a time.

Even if a detailed analysis of privacy policies or related topics was not part of this project, concerns in this area must be raised. Some mobile apps have privacy policies that are most probably translated to German or English by using automated tools. The outcome is pretty poor and, in few cases, difficult to understand.

Furthermore, some of the wearables or their mobile applications are sending data to servers outside of the European Union (e.g. USA, China and others) that are belonging to the manufacturers themselves or other third parties. Beside the encryption on the transport layer (TLS) the data was additionally encrypted by the mobile app or wearable and could therefore not be analysed during this project. This behaviour is not a vulnerability by itself and was therefore not considered during this project.

6 Summary, conclusion and outlook

This report is the result of the project “SiWamed” sponsored by BSI with the objective to develop a cybersecurity review of wearables with medical functionalities and available in Germany. The scope of the study was confined to wearables publicly available and not subject to regulation. Medical devices were therefore not taken into account.

For analysis of the market, the project started with a market survey that supported the growing relevance, popularity and use of wearables. Many consumers are, however, reluctant to use wearables and have concerns specifically about the security of their data and information.

The detailed survey of the wearable market revealed four distinct wearable categories and market segments: smartwatches, basic watches, fitness trackers and smart rings.

Based on the market survey results, ten popular and up-to-date wearable devices were selected as test objects for the following step, the technical security assessment. The assessment was not limited to the wearable device only, but additionally included the connected components mobile app and backend applications which are typically used in combination with the wearable device.

To appreciate the legal and other constraints in the project, the testers defined a customised set of security tests per wearable component. The objective of the selected tests was about gaining an overview about the protections and the security of the wearable device, the connected mobile app and backend application.

Among the ten wearables, the technical assessment uncovered 110 vulnerabilities rated “Medium” or “High”. None of the devices was free of any vulnerabilities.

Considering the sensitivity of data and information processed by the wearables with medical functions, the results raise questions and concerns about the security and protections available, and the importance the majority of vendors and developers attribute to protection of consumers and their data. This is even more critical, if the limited time available for testing, as well the potential consequences of a compromise to the health of users are considered additionally.

The security and protections of wearables and their components must be a major concern for vendors and consumers.

With this report, vendors shall feel encouraged to review the development processes and technical measures to protect health data, as consumer’s confidence is at stake. Consideration of existing security standards, best practises and recommendations, such as

- OWASP Web Security Testing Guide
- OWASP Mobile Application Security Testing Guide
- BSI TR-03107-1: Electronic Identities and Trust Services in E-Government
- BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths
- BSI TR-03161: Security Requirements for eHealth applications

could have avoided most, if not all, vulnerabilities.

Consumers shall be made aware of the potential risks of using wearables and are reminded to be cautious when relying on the data and information provided by wearables.

At the time this study was conducted, the European Union (EU) was proposing a new regulation on “horizontal cybersecurity requirements for products with digital elements”, in short: Cyber Resiliency Act (CRA), which address a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity [9]. The proposal aims, among others, at

- ensuring that manufacturers improve the security of products with digital elements;
- enhancing the transparency of security properties of products with digital elements, and
- enabling businesses and consumers to use products with digital elements securely.

This regulation shall be applicable to products with digital elements that connect to other devices or networks. A product with digital elements is defined as “any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.” Products with digital elements mainly refer to hardware and software, including products whose "intended and foreseeable use includes direct or indirect data connection to a device or network".

Accordingly, it is reasonable to assume that the wearable devices in scope of this study will fall into the category of products with digital elements.

Such product shall be deployed without any exploitable vulnerabilities and shall, based on a risk assessment, protect

- the confidentiality of stored, forwarded or otherwise processed personal and other data, and
- the integrity of stored, forwarded or otherwise processed personal and other data.

According to the CRA, products with digital elements shall be designed, developed and manufactured with a reasonable and appropriate level of cyber security in consideration of the cyber risks.

The testers believe that only a few, if any, of the analysed wearables would meet the requirements and can today be considered as “CRA-ready”.

The framework conditions of this study did not allow for a comprehensive assessment of the wearables. Nevertheless, significant vulnerabilities were found, a factor that does not commensurate with the protection needs of the health data processed. Given the growing popularity of wearables, data security and data protection in the wearable devices as well as the associated mobile apps and backend systems should be regularly and thoroughly reviewed.

7 References

[1] Deutschland Wearables Report 2021, https://store.mintel.com/de/reports/deutschland-wearables-report-2021

[2] gfu, Home Electronic Market Index Quartal 1-4/2022, https://gfu.de/en/market-figures/hemix-2022/

[3] gfu Consumer & Home Electronics GmbH, Pressemitteilung vom 28.04.2022, https://gfu.de/wearables-mit-gesundheitsfunktionen-liegen-im-trend/

[4] Statista.com, Sales of wearables in Germany 2015 to 2022, https://de.statista.com/statistik/daten/studie/551366/umfrage/absatz-von-wearables-in-deutschland/

[5] Statista.com, Turnover of wearables in Germany Deutschland 2014 to 2022, https://de.statista.com/statistik/daten/studie/551388/umfrage/umsatz-mit-wearables-in-deutschland/

[7] Klarna: Shopping Pulse, https://insights.klarna.com/shopping-pulse/

[8] Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/wearables-54088

[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0454

[10] Bitkom Servicegesellschaft mbH: Übersicht Gerätearten zur Berechnung von Garantiebeträgen für Elektrogeräte

[11] EHI Pressemitteilung E-Commerce 2021: Zeit des Wachstums, https://www.ehi.org/presse/e-commerce-2021-zeit-des-wachstums/

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

[13] Open Worldwide Application Security Project - Mobile Application Security Verification Standard (OWASP MASVS), https://mas.owasp.org/MASVS/

[14] Open Worldwide Application Security Project - Mobile Application Security Testing Guide (OWASP MASTG), https://mas.owasp.org/MASTG/

[15] Common Vulnerability Scoring System (CVSS) Version 2.0: https://www.first.org/cvss/v2/guide

Acronyms

Acronym	Meaning
ADB	Android Debug Bridge
AI	Artificial intelligence
AR	Augmented Reality
ECG	Electrocardiography (a medical diagnostic method)
EE	Entertainment Electronics
gfu	Gesellschaft zur Förderung der Unterhaltungselektronik (gfu Consumer & Home Electronics GmbH), Frankfurt/Main
GfK	GfK SE, Nuremberg
GSM	Global System for Mobile Communications
HMAC	Hash-based Message Authentication Code
JTAG	Joint Test Action Group and an industry standard for verifying designs and testing printed circuit boards after manufacture.
JSON	JavaScript Object Notation
JWT	JSON Web Token
MITM	Man/Machine-in-the-Middle
OWASP	Open Worldwide Application Security Forum, see https://owasp.org/
PIN	Personal Identification Number
SDK	Software Development Kit
SIM	Subscriber Identity Module, smartcard for use in mobile handsets
TLS	Transport Layer Security
USB	Universal Serial Bus
VR	Virtual Reality
WIFI	https://en.wikipedia.org/wiki/Wi-Fi
XSS	Cross-Site Scripting – Attack that injects JavaScript code into a website that gets executed client-side

Glossary

Black-Box	Penetration test methodology where the tester does not have any non-public information about the target
CVSS	The Common Vulnerability Scoring System (CVSS) is a free and open industry standard, and provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. See https://www.first.org/cvss/
SSL-Pinning	Technique to bind a specific certificate to an application with the goal to make MITM more difficult
Bluetooth (Pairing)	Wireless protocol to transmit data between nearby devices. Pairing is the mechanism where two Bluetooth communication partners connect to each other and, depending on the pairing mechanism, exchange cryptographic key material
Penetration test	Simulated cyber-attack on one or multiple targets
JTAG	An IEEE industry standard for verifying designs and testing printed circuit boards after manufacture.
XSS	Cross-site scripting means an attack on a website that injects JavaScript code into it which is later executed on the client-side
HMAC	Message authentication involving a cryptographic hash function and a secret cryptographic key.
JWT	JSON data secured with optional signature and/or optional encryption. Often used for authentication.

Appendix A: Unique vulnerabilities

Unique Vulnerability	Rating	Occurences		
		Backend	Mobile app	Wearable device
Account takeover via HMAC secret bruteforce	High	1		
Android certificate transparency	Low		1	
Android Insecure SSL	High		1	
App can be installed on a vulnerable Android version	Medium		5	
Application vulnerable to Janus vulnerability	Low		5	
Arbitrary application installation	Medium			3
Base config is insecurely configured to permit clear text traffic to all domains	Medium		2	
Bluetooth MITM	High			2
Bluetooth pairing sequence without confirmation	High			2
Check path traversal	Medium		1	
Clear text traffic	Medium		3	
Critical permission(s)	Medium		9	
Cross-origin resource sharing: arbitrary origin trusted	Medium	3		
Debug info in SMALI or DEX files	Medium		2	
Hook with graphical overlay	Medium		6	
Information disclosure through extensive logging	Medium		4	
Insecure TLS certificate	Medium	1		
Insufficient hooking detection	Medium		9	
Insufficient root detection	Medium		9	
Insufficient SSL pinning implementation	Medium		9	

Unique Vulnerability	**Rating**	**Occurences**		
		Backend	**Mobile app**	**Wearable device**
Management interfaces accessible on the internet	Medium	1		
Management interfaces accessible on the internet – via plain text http	Medium	1		
Non-standard launch mode of activities	Medium		2	
Pairing PIN bypass	High			3
Pairing to multiple accounts	Medium			3
Repackaging - Setting debuggable flag	Medium		9	
Stripped Debugging Symbols	Medium		1	
TaskAffinity is set for activity	Medium		1	
TinyURL collision on friend/family invite functionality	Medium	1		
Unencrypted communication	Medium	3		
User authentication insufficient on device	Medium			3
User authentication missing on device	Medium			4
Vulnerable JavaScript dependency	Medium	5		
Webview – Debug	Medium		1	