Penetration Test Report

InsoCare

of Dubius Payment Ltd.

EXAMPLE

December 20, 2024

v1.1

Contents

i List of changes

Version	Description	Author	Date
1.0	Report generation	Dominik Sauer	December 19, 2024
1.1	Quality Assurance	QA-Team	December 20, 2024

1 Contact persons

1.1 Contact person Dubius Payment Ltd.

Damian Westcott
CEO

🖂 d.westcott@dubius-payment.com

Dubius Payment Ltd.
71 Peachfield Road
SO53 4NE CHANDLER
United States

1.2 Contact person binsec GmbH

Dominik Sauer
Head of Penetration Testing

☎ +49 69247560713
🖂 ds@binsec.com

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

1.3 About the pentester

Since 2013, Mr. Dominik Sauer has been responsible for the management and implementation of penetration tests at binsec GmbH. He started his career while studying computer science at the Darmstadt University of Applied Sciences and ended his academic career with a very good master's degree in computer science with a specialization in IT security. He also holds the leading certifications in the field of penetration testing and has been an Offensive Security Certified Professional (OSCP) since 2013 and an Offensive Security Certified Expert (OSCE) since 2015.

In addition, he has been a lecturer for teaching at the Darmstadt University of Applied Sciences (HDA) and the TH Mittelhessen University of Applied Sciences (THM) since 2017. For example, he holds courses on penetration testing or digital forensics and supervises theses.

2 Project overview

2.1 Introduction

Dubius Payment Ltd. offers a complete solution for people with diabetes under the name InsoCare. InsoCare consists of the following three components:

- InsoPump
- InsoSense
- InsoApp

Both InsoPump, the insulin pump, and InsoSense, the associated sensor, communicate with the InsoApp via Bluetooth Low Energy. InsoApp is available for both Android and iOS. InsoApp was subjected to a separate pentest.

2.2 Basic conditions

The penetration test was conducted between June 5, 2024 and June 7, 2024 performed as an internal grey box test, without using aggressive attacking techniques such as DDoS attacks. The complete classification is illustrated in chapter 5.1. The general pentest approach is described in chapter 5.2.

2.3 Scope

Only the InsoPump and InsoSense were the subject of this pentest - the InsoApp version 1.2b was only made available to the pentester to check the Bluetooth communication.

2.4 Performed tests

The following pentest tasks were performed on the systems and applications described previously. This list was automatically generated by binsec GmbH's documentation tool.

Target → Hardware: InsoPump

Result	Task: Information gathering (passive, external resources)	Findings
✔	Identification of accessible Interfaces	-

Target → Hardware: InsoPump · UART: Debug-Interface

Result	Task: Information gathering (active, test objects)	Findings
✔	Identify UART Ports	-
✔	Check if it is possible to dump the firmware	-

Target → Hardware: InsoPump · Bluetooth LE: InsoPump <--> InsoApp

Result	Task: Information gathering (passive, external resources)	Findings
✔	Identification of the Bluetooth version	-
✘	Review of Privacy Features	Page 12
Result	Task: Information gathering (active, test objects)	Findings
✔	Analysis of data communication	-
Result	Task: Cryptography	Findings
✘	Analysis of the connection setup	Page 10
Result	Task: Input validation (e.g. Injection, XSS)	Findings
✔	Automated checking of input validation via Fuzzing	-
Result	Task: Vulnerability identification	Findings
✔	Check for low level attacks leading to a compromised connection	-
✘	Check for low level attacks leading to crashed device	Page 11
✔	Check for low level attacks leading to a deadlock	-

Target → Hardware: InsoSense

Result	Task: Information gathering (passive, external resources)	Findings
✔	Identification of accessible Interfaces	-

Target → Hardware: InsoSense · Bluetooth LE: InsoSense <--> InsoApp

Result	Task: Information gathering (passive, external resources)	Findings
✔	Identification of the Bluetooth version	-
✘	Review of Privacy Features	Page 12
Result	Task: Information gathering (active, test objects)	Findings
✔	Analysis of data communication	-
Result	Task: Cryptography	Findings
✘	Analysis of the connection setup	Page 10
Result	Task: Input validation (e.g. Injection, XSS)	Findings
✔	Automated checking of input validation via Fuzzing	-
Result	Task: Vulnerability identification	Findings
✔	Check for low level attacks leading to a compromised connection	-
✘	Check for low level attacks leading to crashed device	Page 11
✔	Check for low level attacks leading to a deadlock	-

3 Management overview

3.1 Summary

The penetration test was conducted between June 5, 2024 and June 7, 2024. During it 4 vulnerabilities were identified which were combined into 3 findings and subjected to an initial risk assessment. As result there is no finding that requires immediate action and 2 findings that require action. The finding of category note is to be understood as a suggestion to increase the security level.

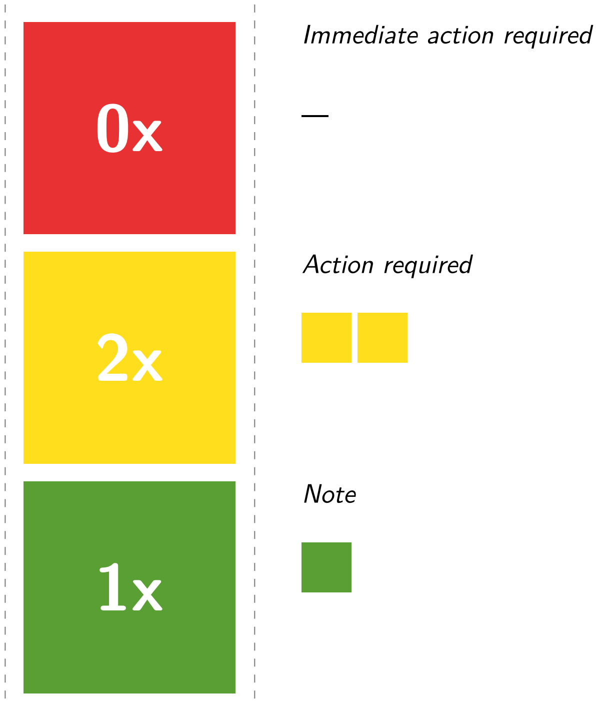


Fig. Risk Overview of Findings

During the penetration test, several vulnerabilities requiring action were identified, both of which affect the Bluetooth LE connection of both the InsoPump and the InsoSense. Firstly, the connection between InsoPump and InsoSense is based on outdated Bluetooth LE security features and is therefore susceptible to man-in-the-middle attacks. Secondly, the Bluetooth LE chip built into the InsoPump is susceptible to already known vulnerabilities, which means that the InsoPump can be crashed by an attacker.

3.2 List of findings

1 ⬜🟨⬜

Not fixed: *Data Transmission*

An outdated Bluetooth pairing method is used for which vulnerabilities are already known. See page 10.

System: InsoPump, InsoSense

2 ⬜🟨⬜

Not fixed: *Data Transmission*

The InsoPump can be crashed via a manipulated Bluetooth connection. See page 11.

System: InsoPump

3 ⬜⬜🟩

Not fixed: *Misconfiguration*

When switched on, users of the insulin pump can be tracked. See page 12.

System: InsoPump

4 Technical report

4.1 Use of outdated Bluetooth pairing methods

◼ action required
🟨 Damage: medium
◼ Occurrence: medium

Finding #1 **Not fixed**

The encrypted connection setup in Bluetooth Low Energy is realized via so-called 'pairing'. The pairing methods of versions 4.0 and 4.1 have been grouped under 'legacy' since the release of version 4.2 in 2014 and are susceptible to brute force attacks[1]. In detail, this means that an attacker who is able to record the connection setup via Bluetooth LE can bypass the encryption of the connection and gain access to any sensitive data.

Recommendation

Instead of the outdated pairing method, 'Secure Connections' pairing should be used.

[1] `https://www.sciencedirect.com/science/article/pii/S1389128621005697#sec4.5`

4.2 InsoPump can be crashed via BLE

■ action required

🟨 Damage: medium

■ Occurrence: medium

Finding #2

Not fixed

Under the name 'SweynTooth', a total of 14 vulnerabilities were identified in various Bluetooth LE implementations in 2020[2]. These vulnerabilities were divided into three groups: Crash, Deadlock and Security Bypass. As can be seen in the following listing, the insulin pump is vulnerable to the 'Invalid Channel Map' attack, which causes the device to crash:

```
$ python2.7 invalid_channel_map.py /dev/ttyACM0 **:**:**:**:**:**
Serial port: /dev/ttyACM0
Advertiser Address: **:**:**:**:**:**
TX ---> BTLE_ADV / BTLE_SCAN_REQ
Waiting advertisements from **:**:**:**:**:**
**:**:**:**:**:**: BTLE_ADV / BTLE_ADV_IND Detected
TX ---> BTLE_ADV / BTLE_CONNECT_REQ
Malformed connection request was sent
TX ---> BTLE_ADV / BTLE_SCAN_REQ
TX ---> BTLE_ADV / BTLE_SCAN_REQ
No advertisement from **:**:**:**:**:** received
The device may have crashed!!!
Capture saved in logs/invalid_channel_map.pcap
```

The value of the 'Channel Map' specifies the channels to be used when establishing a BLE connection, whereby the Bluetooth specification prescribes a minimum number of 2 channels. If the value is set to 0 instead, this causes the device to crash. The insulin pump is ready for use again after a few seconds, even without external intervention.

Recommendation

If an update is available from the BLE SoC manufacturer concerned, this should be used.

[2] https://asset-group.github.io/disclosures/sweyntooth/

4.3 Missing privacy feature

⬜ note

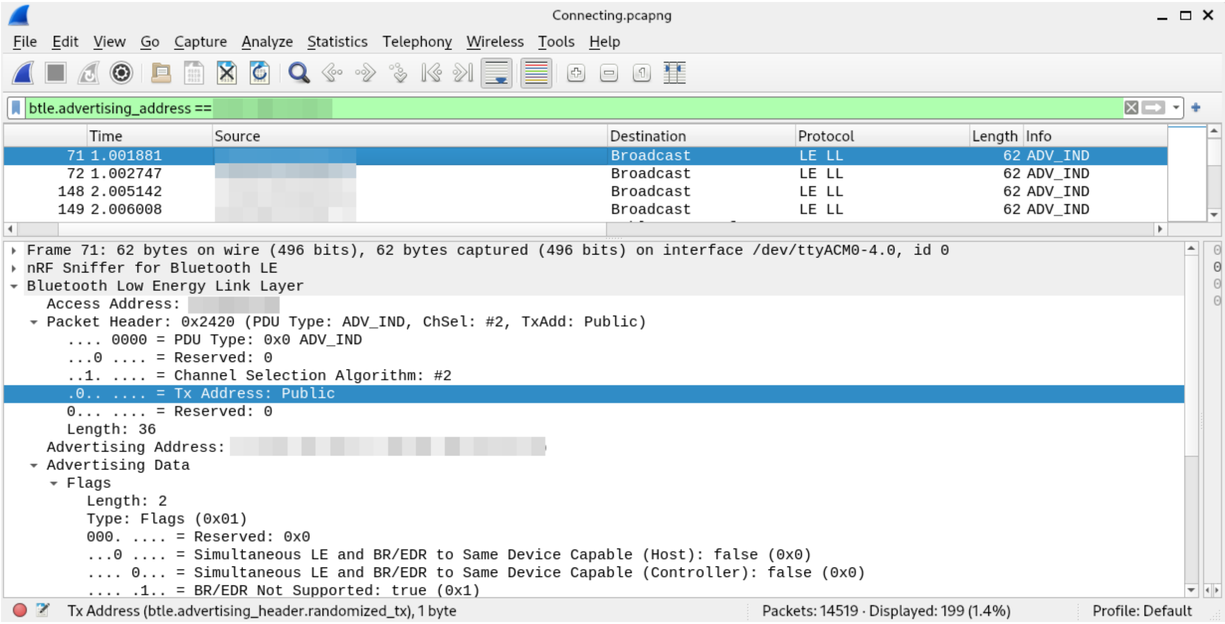
⬜ Damage: warning

🟩 Occurrence: high

Finding #3 **Not fixed**

Bluetooth Low Energy (BLE) offers various privacy features to ensure the security and privacy of users. One of the central functions is the privacy feature, which aims to disguise the identity of devices to reduce traceability.[3]

This feature is not used in the advertisements of the insulin pump. As the following screenshot shows, advertisements are sent with a so-called 'Public Address':


Connecting.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

btle.advertising_address == [redacted]

```
  Time         Source        Destination  Protocol  Length Info
 71 1.001881   [redacted]    Broadcast    LE LL       62 ADV_IND
 72 1.002747                 Broadcast    LE LL       62 ADV_IND
148 2.005142                 Broadcast    LE LL       62 ADV_IND
149 2.006008                 Broadcast    LE LL       62 ADV_IND
```

```
› Frame 71: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface /dev/ttyACM0-4.0, id 0
› nRF Sniffer for Bluetooth LE
⌄ Bluetooth Low Energy Link Layer
    Access Address: [redacted]
  ⌄ Packet Header: 0x2420 (PDU Type: ADV_IND, ChSel: #2, TxAdd: Public)
      .... 0000 = PDU Type: 0x0 ADV_IND
      ...0 .... = Reserved: 0
      ..1. .... = Channel Selection Algorithm: #2
      .0.. .... = Tx Address: Public
      0... .... = Reserved: 0
      Length: 36
    Advertising Address: [redacted]
  ⌄ Advertising Data
    ⌄ Flags
        Length: 2
        Type: Flags (0x01)
        000. .... = Reserved: 0x0
        ...0 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x0)
        .... 0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x0)
        .... .1.. = BR/EDR Not Supported: true (0x1)
```

Tx Address (btle.advertising_header.randomized_tx), 1 byte   Packets: 14519 · Displayed: 199 (1.4%)   Profile: Default

While the device is switched on and sending advertisements, users of the device can be tracked.

Recommendation

The Privacy Feature[4] should be implemented for the insulin pump.

[3] 'A survey on Bluetooth Low Energy security and privacy', 3.1.5. privacy features (https://doi.org/10.1016/j.comnet.2021.108712)

[4] Bluetooth Core Specification Version 6.0, Vol 1, Part A, 5.4.5 'Privacy Feature'

5 Appendix A

5.1 Classification details

In cooperation with Dubius Payment Ltd., the following classification variant was agreed as the approach: The penetration test was performed as an internal grey box test, without using aggressive attacking techniques such as DDoS attacks.

Pursuant to the study "Implementation Concept for Penetration Tests" by the German Federal Office for Information Security (BSI), binsec GmbH used the following classification for this penetration test:

Test Type	**Black-Box**	[✓ **Grey-Box**]	**White-Box**	
Aggressiveness	**passive**	**cautious**	[✓ **calculated**]	**aggressive**
Scope	**full**	[✓ **limited**]	**focused**	
Aproach	**covert**	[✓ **overt**]		
Technique	**Internet**	[✓ **physical access**]	**Social engineering**	
Starting Point	**external**	[✓ **internal**]		

5.2 Procedure for Medical Devices

The Medical Device Regulation (MDR) requires the verification and validation of the security of medical devices and software. The Medical Device Coordination Group states in its guide to cybersecurity for medical devices that the primary means of security verification and validation is testing.

The procedure for a penetration test for a medical device, usually consisting of one or more hardware devices and associated software, is usually done on a case-by-case basis due to the different use cases of these medical devices and their functionality. The key questions for a penetration test of a medical device are usually:

- Can the patient's health be negatively affected by direct manipulation of the device?
- Can measured data be manipulated so that the patient is harmed due to incorrect or lack of treatment?
- Is the patient's health data adequately protected in the processing IT systems?

Medical devices often consist of a technical interaction of sensors/measuring devices, an embedded Linux OS with wireless data transmission via Bluetooth/RFID/WIFI, while data processing is carried out on Windows computers, smartphones and/or in the cloud.

The procedure, or the specific attack vectors to be tested, are therefore initially discussed with the customer and usually include a test of the wireless data transmission, opening the device to identify further attack vectors and, depending on the individual case, testing of web applications and APIs.

5.3 Risk assessment

Binsec GmbH considers the term “risk“ to mean a combination of the probability of occurrence of a vulnerability (or the likelihood of its exploitation) and the possible extent of damage. The probability of occurrence or the probability of exploitation of a security gap in IT systems essentially depends on these factors:

- How easily can the vulnerability be identified? (Visibility)
- Are there any exploits for this vulnerability available, or is the attacker required to have a certain level of knowledge to exploit them? (Exploitability)
- Does the exploitation require special rights? (Privilege Escalation)
- Is a combination with other security holes required? (Vulnerability Chaining)
- Is human interaction necessary for the vulnerability? (Social Engineering)

The following classifications are decisive for the possible extent of damage:

1. Financial damage
2. Complete compromising of the system
3. Violation of security objectives related to data or user accounts:
    a) Confidentiality
    b) Availability
    c) Integrity
4. Bypassing of security measures
5. Information disclosure

Taking into account both the probability of occurrence and the potential extent of damage, the penetration tester makes a subjective assessment of the risk for each vulnerability found. We recommend taking an own assessment of the vulnerabilities.

The assessment is subject to the following classification:

occurrence probability	
high	The vulnerability is obvious or exploits are freely available.
medium	The vulnerability can be identified in a reasonable amount of time; exploits may need to be adapted.
low	The vulnerability is difficult to find and may require permissions or the exploitation of other vulnerabilities.

extent of damage	
critical	Complete compromising of the system.
high	Violation of security objectives concerning information or IT systems.
medium	Bypassing of security measures.
low	Preparation for exploitation of other vulnerabilities as part of a sustained attack.
warning	Information disclosure.

The risk classification entails a priority for action.

		extent of damage				
		warning	low	medium	high	critical
occurrence probability	high	🟩	🟨	🟥	🟥	🟥
	medium	🟩	🟨	🟨	🟥	🟥
	low	🟩	🟩	🟨	🟨	🟥

🟩 note 🟨 action required 🟥 immediate action required

5.4 About the binsec GmbH

We are a company that specializes in IT penetration testing, located at Frankfurt am Main, Germany. Since 2013, carrying out technical security analyses of IT infrastructures, web applications, APIs, mobile apps (Android / iOS), etc. has been the core of our daily work. As an owner-managed company, the long-term satisfaction of our customers is of great importance. The certifications of our employees, the teaching activities at universities and our pentesting experience speak for themselves.

BETTER PENTESTING
NO NONSENSE

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

✉ info@binsec.com
☎ +49 69 2475607-0

Managing Director:	Patrick Sauer
Authorised Officers:	Dominik Sauer, Florian Zavatzki

Commercial Register:	Frankfurt a.M. HRB 97277
VAT ID no.:	DE290966808