

## **UK PSTI Compliance Assessment**

**The Product Security and Telecommunications  
Infrastructure (Security Requirements for Relevant  
Connectable Products) Regulations 2023**

IMOO INTERNATIONAL PTE. LTD  
Watch phone Model W2432AO

|                |               |
|----------------|---------------|
| Author         | Chen, Yi Cong |
| Version        | 1.0           |
| Date           | 26 Aug 2025   |
| Status         | Released      |
| Classification | Confidential  |

**Project information**

|                 |                      |
|-----------------|----------------------|
| Project Manager | <i>Deng, Estella</i> |
| Project Code    | <i>UL4791875048</i>  |
| Classification  | <i>Confidential</i>  |

**Customer information**

|                     |                                    |
|---------------------|------------------------------------|
| Customer Name       | <i>IMOO INTERNATIONAL PTE. LTD</i> |
| Product Name        | <i>Watch phone Model W2432AO</i>   |
| Hardware Version(s) | <i>GLI32-M-0</i>                   |
| Software Version(s) | <i>1.1.0</i>                       |
| Customer Contact    | <i>timothy@imoo.com</i>            |

UL Verification Services (Guangzhou) Co., Ltd  
Building A1, 5F  
Nansha Science and Technology Innovation Center, No.25  
South Huanshi Avenue, Nansha district  
Guangzhou / Guangdong, 511458

E-mail [info@ul.com](mailto:info@ul.com)  
Website [www.ul.com](http://www.ul.com)

**Version History**

| Version | Date        | Author        | Nature of Amendment |
|---------|-------------|---------------|---------------------|
| 0.1     | 26 Aug 2025 | Chen, Yi Cong | Initial Draft       |
| 1.0     | 27 Aug 2025 | Chen, Yi Cong | Released            |

# Management Summary

This document presents the results of the Product Security and Telecommunications Infrastructure Act 2022 (referred to as PSTI Act, or Act) compliance assessment of the Watch phone W2432AO product produced by IMOO INTERNATIONAL PTE. LTD(referred to as IMOO). The assessment was conducted in accordance with the UK PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023 (Regulations). The conditions for deemed compliance with security requirements were considered (SCHEDULE 2).

The Watch phone W2432AO is a smartwatch designed for children to facilitate communication with their parents. The product has six external physical interfaces. The has a Wi-Fi interface, a Bluetooth interface, and a cellular network interface, supporting BLE communication and TLS secure communication.

The assessment was based on customer-provided documentation (both public and proprietary), a product sample Watch phone W2432AO for functional testing, and direct communications. It was found that the Watch phone W2432AO product complies with all the relevant requirements of the regulations. This includes security requirements for:

- Passwords (ETSI EN 303 645 Provisions 5.1-1 and 5.1-2)
- Information on how to report security issues (Provision 5.2-1)
- Information on minimum security update periods (Provision 5.3-13)

Overall, the Watch phone W2432AO product complies with the UK PSTI Regulations 2023.

# Table of Contents

|                                                                                |           |
|--------------------------------------------------------------------------------|-----------|
| <b>MANAGEMENT SUMMARY .....</b>                                                | <b>4</b>  |
| <b>1     PRODUCT DESCRIPTION .....</b>                                         | <b>6</b>  |
| 1.1     Characteristics .....                                                  | 6         |
| 1.2     Product Image.....                                                     | 7         |
| 1.3     Scope.....                                                             | 7         |
| 1.4     Intended audience .....                                                | 7         |
| 1.5     Samples .....                                                          | 8         |
| <b>2     UK PSTI – TESTING PROCESS .....</b>                                   | <b>9</b>  |
| 2.1     Security Provisions .....                                              | 9         |
| <b>3     SECURITY ASSESSMENT SUMMARY .....</b>                                 | <b>10</b> |
| 3.1     Summary of results .....                                               | 10        |
| 3.2     Security Assessment Results Breakdown .....                            | 11        |
| 3.2.1 1.1 Passwords (Provision 5.1-1) .....                                    | 11        |
| 3.2.2 1.2 Passwords (Provision 5.1-2) .....                                    | 11        |
| 3.2.3 2 Information on how to report security issues (Provision 5.2-1).....    | 12        |
| 3.2.4 3 Information on minimum security update periods (Provision 5.3-13)..... | 12        |
| <b>REFERENCES .....</b>                                                        | <b>13</b> |
| <b>A.1   NON-FACTORY PASSWORD .....</b>                                        | <b>14</b> |
| <b>A.2   VULNERABILITY DISCLOSURE POLICY .....</b>                             | <b>17</b> |
| <b>A.3   SUPPORT PERIOD.....</b>                                               | <b>18</b> |

# 1 Product Description

## 1.1 Characteristics

The product that UL tested is described in Table 1 and can be seen depicted in Figure 1.

| Component             | Designation                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Name of Laboratory    | UL Verification Service (Guangzhou) Co., Ltd                                                                                                        |
| Address of Laboratory | Building A1, 5F<br>Nansha Science and Technology Innovation Center, No.25<br>South Huanshi Avenue, Nansha district<br>Guangzhou / Guangdong, 511458 |
| Location of Testing   | Same as the Address of the Laboratory                                                                                                               |
| Name of Applicant     | IMOO INTERNATIONAL PTE. LTD                                                                                                                         |
| Address of Applicant  | Room 1102, Building 1, No. 28, Dongmen Middle Road, Chang'an<br>Town, Dongguan City, Guangdong Province, 523850, China                              |
| Contact of Applicant  | timothy@imoo.com                                                                                                                                    |
| Product Designation   | Watch phone Model W2432AO                                                                                                                           |
| Hardware Version      | GLI32-M-0                                                                                                                                           |
| Software Version      | 1.1.0                                                                                                                                               |
| Date of Testing       | 2025.8.20-2025.8.25                                                                                                                                 |
| Test Methodology      | PSTI Regulations 2023; ETSI EN 303 645 V2.1.1 (2020-06)                                                                                             |
| Test Equipment Used   | DELL P135G, TP-Link Router AX5400                                                                                                                   |

**Table 1 – Project Characteristics**

## 1.2 Product Image

The Target of Evaluation (TOE) can be seen depicted in Figure 1



Figure 1 TOE

## 1.3 Scope

This report presents an evaluation of the security compliance of IMOO INTERNATIONAL PTE. LTD product with the PSTI Act, which mandates minimum cybersecurity capabilities for “internet-connectable products” (as defined by the Act). The scope of this report includes IMOO INTERNATIONAL PTE. LTD Watch phone W2432AO, as described above. As per Schedule 2 of the Regulations, additional expectations beyond the EN 303 645 Provisions are assessed. A high-level architecture of the IoT Ecosystem can be seen depicted in Figure 2.

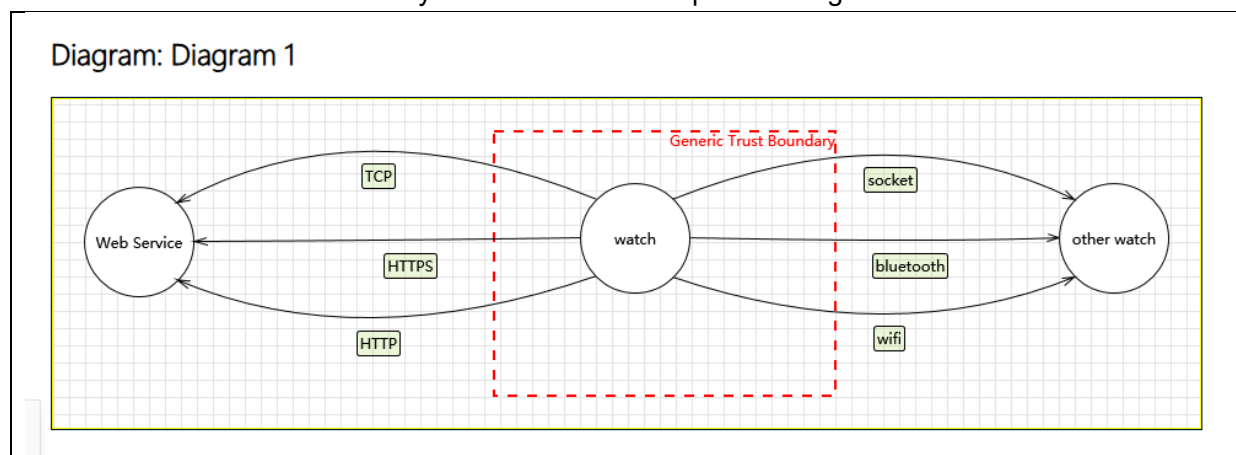


Figure 2 IoT ecosystem

## 1.4 Intended audience

This document is written for IMOO INTERNATIONAL PTE. LTD's technical, software development, and business teams.

## 1.5 Samples

The samples provided by IMOO INTERNATIONAL PTE. LTD can be seen depicted in Table 2.

| No. | Type    | Serial Number | Remarks                                                |
|-----|---------|---------------|--------------------------------------------------------|
| 1   | W2432AO | 6032G530005AE | Hardware Version: GLI32-M-0<br>Software Version: 1.1.0 |

**Table 2 – Product Details**

## 2 UK PSTI – Testing Process

### 2.1 Security Provisions

Using the testing approach described in ETSI EN 303 645 standard and supporting guidance, the Provisions referenced in the Regulations are considered Mandatory and In-Scope. The security regulations used for the evaluation against the UK PSTI compliance assessment can be seen listed in Table 3.

NOTE: The Act and Regulations define additional requirements beyond the wording from EN 303 645:2020. All additional requirements are noted in the summary of findings and are also mandatory for passing a regulation.

| Regulation | Title                                          | Provision | M |
|------------|------------------------------------------------|-----------|---|
| 1          | Passwords                                      | 5.1-1     | X |
|            |                                                | 5.1-2     | X |
| 2          | Information on how to report security issues   | 5.2-1     | X |
| 3          | Information on minimum security update periods | 5.3-13    | X |

Table 3 – ETSI EN 303 645 provisions for Regulations of PSTI

## 3 Security Assessment Summary

UL Solutions lab engineers and appropriate staff reviewed the information provided by the vendor. If the Result column shows Pass, the device is considered to be compliant with such Regulation. The details for each requirement are itemized in Section 3.2.

### 3.1 Summary of results

The summary of results is presented in Table 4.

| Regulation | Title                                          | Provision # | Result |
|------------|------------------------------------------------|-------------|--------|
| 1          | Passwords                                      | 5.1-1       | Pass   |
|            |                                                | 5.1-2       | N/A    |
| 2          | Information on how to report security issues   | 5.2-1       | Pass   |
| 3          | Information on minimum security update periods | 5.3-13      | Pass   |

Table 4 - Security Assessment Summary for Mandatory Items.

## 3.2 Security Assessment Results Breakdown

Each specific regulation is listed in this section, along with a summary of findings.

### 3.2.1 1.1 Passwords (Provision 5.1-1)

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                   |              |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|--------------|
| <b>Security Capability Description</b> | Passwords in scope, used in any state other than the factory default, must be unique per product or defined by the user of the product.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                   |              |
| <b>Summary of Findings</b>             | <p><b>1. Lock Screen password</b><br/>The evaluator tested and confirmed that the product could be set with a lock screen password. The evaluator confirmed that this password was defined by the user when setting the lock screen password for the first time, as shown in Figure 3.</p> <p><b>2. Wi-Fi password</b><br/>The evaluator tested and confirmed that the product could connect to the external access point (AP). When connecting to a Wi-Fi network that required password authentication, a password input box showed up as shown in Figure 4. The evaluator confirmed that the Wi-Fi password wasn't defined on the product itself, but rather on the external Wi-Fi AP. The evaluator also confirmed that there was no open port, as shown in Figure 5.</p> <p><b>3. BLE pairing code</b><br/>The evaluator tested and confirmed that when the external device attempted to connect to the product via Bluetooth, PIN code authentication was required, as shown in Figure 7. This code was generated randomly and was different each time the connection was made.</p> <p><b>4. System Local Port</b><br/>The evaluator tested and confirmed that when the product was connected to the PC via the special wire for charging, access to the local system could not be accessed, as shown in Figure 8.</p> |                                   |              |
| <b>RESULT</b>                          | Pass                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>Detailed Results Reference</b> | Appendix A.1 |

### 3.2.2 1.2 Passwords (Provision 5.1-2)

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                   |     |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-----|
| <b>Security Capability Description</b> | <p>Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.</p> <p>Password generation mechanisms which fail:</p> <ul style="list-style-type: none"> <li>a) based on incremental counters;</li> <li>b) based on or derived from publicly available information;</li> <li>c) based on or derived from unique product identifiers, such as serial numbers, unless this is done using an encryption method, or keyed hashing algorithm, that is accepted as part of good industry practice;</li> <li>d) otherwise guessable in a manner unacceptable as part of good industry practice.</li> </ul> |                                   |     |
| <b>Summary of Findings</b>             | Testing confirmed that there was no pre-installed password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                   |     |
| <b>RESULT</b>                          | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Detailed Results Reference</b> | N/A |

### 3.2.3 2 Information on how to report security issues (Provision 5.2-1)

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Security Capability Description</b> | <p>The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum:</p> <ul style="list-style-type: none"> <li>• contact information for the reporting of issues; and</li> <li>• information on timelines for:               <ol style="list-style-type: none"> <li>1) initial acknowledgement of receipt; and</li> <li>2) status updates until the resolution of the reported issues.</li> </ol> </li> </ul> <p>Additional mandates: the information must be accessible, clear and transparent</p> <ol style="list-style-type: none"> <li>(a) without prior request for such information being made;</li> <li>(b) in English;</li> <li>(c) free of charge; and</li> <li>(d) without requesting the provision of a person's personal information.</li> </ol> <p><b>NOTE:</b> This regulation applies to hardware, software installed on the device or required to be installed, software used for remote access (eg. Phone apps) and cloud service software used for or in connection with the product.</p> |
| <b>Summary of Findings</b>             | <p>Testing verified the following URL meets all elements of this requirement: The evaluator checked the "SECURITY MEASURES" item on the URL <a href="https://uk.imooostore.com/pages/psti-statement-of-compliance">https://uk.imooostore.com/pages/psti-statement-of-compliance</a>. The contact information was shown in Figure 9, which also implied that the manufacturer didn't need the personal information of the reporter. The manufacturer stated that they acknowledged any vulnerability reports or concerns within 7 calendar days. When applicable, they shared vulnerability reports and updates with affected parties within 7 to 14 days, with weekly updates until the issues are resolved.</p>                                                                                                                                                                                                                                                                                                                                                      |
| <b>RESULT</b>                          | <div>Pass</div> <div><b>Detailed Results Reference</b></div> <div>Appendix A.2</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### 3.2.4 3 Information on minimum security update periods (Provision 5.3-13)

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Security Capability Description</b> | <p>The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the "defined support period".</p> <p>Additional mandates: the information must be accessible, clear and transparent</p> <ol style="list-style-type: none"> <li>(a) without prior request for such information being made;</li> <li>(b) in English;</li> <li>(c) free of charge;</li> <li>(d) without requesting the provision of a person's personal information; and</li> <li>(e) in such a way that is understandable by a reader without prior technical knowledge.</li> </ol> <p><b>NOTE:</b> This regulation applies to hardware, software installed on the device or required to be installed, software used for remote access (eg. Phone apps) and cloud service software used for or in connection with the product.</p> |
| <b>Summary of Findings</b>             | <p>Testing verified the following URL meets all elements of this requirement: The evaluator checked the file "Product Security Update Period.pdf" and found the end date of the support period of this product was September 1st, 2027. The manufacturer stated that they would update the update period information of the model X10 on the URL <a href="https://les.mitsubishielectric.co.uk/psti-statement-of-compliance">https://les.mitsubishielectric.co.uk/psti-statement-of-compliance</a> later, as shown in Figure 10. The evaluator confirmed that this implementation was feasible.</p>                                                                                                                                                                                                                                 |
| <b>RESULT</b>                          | <div>Pass</div> <div><b>Detailed Results Reference</b></div> <div>Appendix A.3</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## References

| Ref. | Title                              | Date    |
|------|------------------------------------|---------|
| [1]  | Product Security Update Period.pdf | 08-2025 |

## A.1 Non-factory Password

### 1. Lock screen password

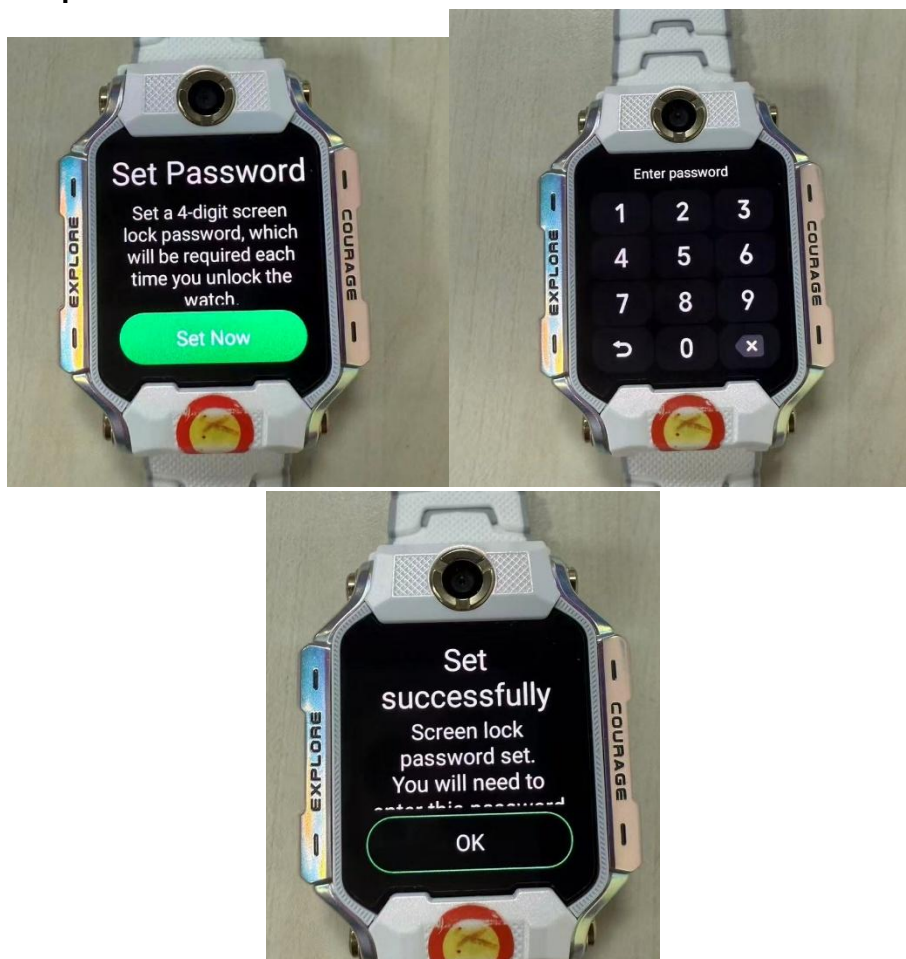


Figure 3 Lock Screen Password Setting Process

### 2. Wi-Fi password



Figure 4 Wi-Fi Password Input Box

The evaluator used Nmap to scan the open ports on the product, found that there was no open TCP port. The UDP port scan has been running for over 48 hours. From the UDP port scan performance, the evaluator believed that there was no open UDP port.

```
Host is up (0.13s latency).
All 1000 scanned ports on 172.16.1.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 88:45:F0:27:2B:F2 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   133.15 ms 172.16.1.101

NSE: Script Post-scanning.
Initiating NSE at 17:51

# nmap -v -sT -p- 172.16.1.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 18:51 CST
Initiating ARP Ping Scan at 18:51
Scanning 172.16.1.101 [1 port]
Completed ARP Ping Scan at 18:51, 0.07s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating Connect Scan at 18:51
Scanning 172.16.1.101 [65535 ports]
Completed Connect Scan at 18:51, 31.87s elapsed (65535 total ports)
Nmap scan report for 172.16.1.101
Host is up (0.023s latency).
All 65535 scanned ports on 172.16.1.101 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)
MAC Address: 88:45:F0:27:2B:F2 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 32.02 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

UDP Scan Timing: About 13.71% done; ETC: 14:40 (55:21:24 remaining)
UDP Scan Timing: About 14.07% done; ETC: 18:40 (58:33:58 remaining)
UDP Scan Timing: About 14.48% done; ETC: 22:59 (61:58:31 remaining)
UDP Scan Timing: About 14.95% done; ETC: 03:38 (65:36:00 remaining)
UDP Scan Timing: About 15.50% done; ETC: 08:42 (69:27:29 remaining)
UDP Scan Timing: About 16.14% done; ETC: 14:14 (73:34:09 remaining)
UDP Scan Timing: About 16.92% done; ETC: 20:21 (77:57:29 remaining)
UDP Scan Timing: About 17.88% done; ETC: 03:10 (82:39:04 remaining)
```

Figure 5 Nmap Scan

### 3. Bluetooth pairing code

When the evaluator tried to connect to the product via Bluetooth using the PC, in the pairing process, the PIN code was required.

```
[X10]> info
Device 88:45:F0:27:2B:F3 (public)
  Name: X10
  Alias: X10
  Class: 0x005a020c (5898764)
  Icon: phone
  Paired: yes
  Bonded: yes
  Trusted: no
  Blocked: no
  Connected: yes
  LegacyPairing: no
  UUID: Audio Source (0000110a-0000-1000-8000-00805f9b34fb)
  UUID: A/V Remote Control Target (0000110c-0000-1000-8000-00805f9b34fb)
  UUID: A/V Remote Control (0000110e-0000-1000-8000-00805f9b34fb)
  UUID: Headset AG (00001112-0000-1000-8000-00805f9b34fb)
  UUID: Handsfree Audio Gateway (0000111f-0000-1000-8000-00805f9b34fb)
  UUID: PnP Information (00001200-0000-1000-8000-00805f9b34fb)
  UUID: Generic Access Profile (00001800-0000-1000-8000-00805f9b34fb)
  UUID: Generic Attribute Profile (00001801-0000-1000-8000-00805f9b34fb)
  Modalias: bluetooth:v001Dp1200d1436
```

Figure 6 Bluetooth Connection Via Computer

```
[bluetoothctl]> pair 88:45:F0:27:2B:F3
Attempting to pair with 88:45:F0:27:2B:F3
hci0 device_flags_changed: 88:45:F0:27:2B:F3 (BR/EDR)
  supp: 0x00000001 curr: 0x00000000
hci0 88:45:F0:27:2B:F3 type BR/EDR connected eir_len 10
[CHG] Device 88:45:F0:27:2B:F3 Connected: yes
Request confirmation
[agent] Confirm passkey 396978 (yes/no):
```

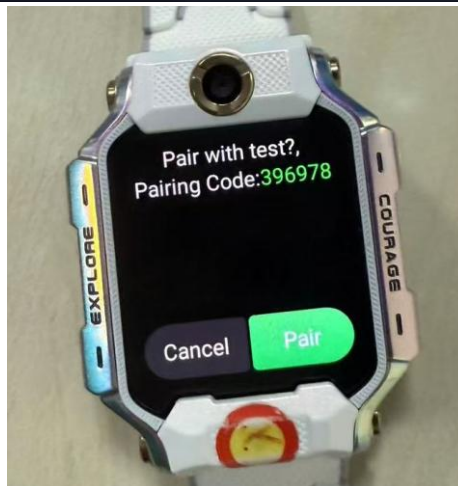


Figure 7 Pairing With PIN Code

#### 4. USB-A Port

When the evaluator tried to access the local system of the product, and found that no port was recognized.



Figure 8 Can Not Access The Local System

## A.2 Vulnerability Disclosure Policy

### SECURITY MEASURES

We implement robust physical, administrative, and technical measures to safeguard the integrity and security of your Personal Data. IMOO employs a comprehensive suite of security strategies to ensure the protection of user and device data. For device access, our proprietary algorithms facilitate data isolation, access authentication, and authorization. In terms of data communication, we utilize secure algorithms, dynamic key-based encryption protocols, and commercial-grade encryption to ensure data confidentiality. For data processing, we apply stringent data filtering, validation, and comprehensive auditing. All user confidential information is securely encrypted during storage. Should you suspect any security issues in your interactions with us, please promptly notify us via sending e-mail to [support@imoostore.com](mailto:support@imoostore.com).

We strive to deliver continuous security updates for our IoT products, encompassing the latest patches, vulnerability fixes, and enhancements. These updates will be supported for a minimum of 1 year from the product launch date. The support period will not be shortened but may be extended as needed. You can reach out to us to inquire about the latest security updates, support duration, or device eligibility for updates.

Please note that our security updates, policies, and devices are subject to periodic review and may change. We commit to acknowledging any vulnerability reports or concerns within 7 calendar days. When applicable, we will share vulnerability reports and updates with affected parties within 7 to 14 days, with weekly updates until the issues are resolved.

Figure 9 Timeline

## A.3 Support Period

### Product Security Update Period

IMOO prioritizes the security of its products and services as a fundamental aspect of our commitment to our users. To uphold this commitment, we diligently provide timely updates to system security patches. These updates are essential to safeguard the information of every device and user, ensuring a secure experience for all. For the IMOO Watch Phone, we pledge to provide security updates for a minimum of one (1) year.

Our users could submit vulnerability report on **Official After-sales Channels** to report any security issues to IMOO.

| Product Name         | End Date of Period |
|----------------------|--------------------|
| imoo watch phone Z1  | 01-July-2025       |
| imoo watch phone Z7  | 01-August-2025     |
| imoo openbuds E5     | 01-March-2026      |
| imoo watch phone Z3  | 01-Sep-2027        |
| imoo watch phone X10 | 01-Sep -2027       |

#### Disclaimer:

1. The information provided on this page is for reference only. The specific details of security updates and applicable device models are subject to the actual updates received by the device.
2. Operating system upgrades may lead to delays in receiving security updates for the current month. However, the new OS version will incorporate the latest security patches.
3. We strive to provide security updates for all applicable device models to the best of our ability. However, actual delivery times may vary depending on the country (region) or model.
4. Certain patches provided by chip suppliers may not be included in the security updates for the current month. Nevertheless, once these patches are available for delivery, they will be included in the upcoming release of security updates.

Figure 10 Support Period