# IoT Test Report for Security Management, Threat and Risk Assessment

**Author:** Serafim Ciobanu

## Main details

This document will represent a report in which I will present my findings, based on the ETSI 303 645 standard on cybersecurity for consumer IoT devices, where the object of testing will be a smart watch **CMF Watch Pro 2**, which falls under the category of IoT devices.

Small disclaimer, I will not be able to test every aspect specified in paragraph 5 of the standard. Also, not every single aspect falls for the device itself, as it does not have very extensive functionality.

## Cyber security provisions for consumer IoT

|  |  |  |
| --- | --- | --- |
| Subparagraph | Description | Test results |
| 5.1 – No universal default passwords  (Compliant) | The device should have a method of authentication that will be unique for every single device. This can be done in multiple ways, one of which can be the user, creating separate accounts for the device/software. | The device itself does not have any authentication method on itself but has a special software **CMF Watch** that already requires the user to create an account (so uniquely created) for the usage of additional functionalities of the smart watch.  This software is also used to pair the phone with the watch, which is the first thing being asked on first start of the watch. Additionally, the watch will provide a special code to make this connection, shown to the user.  Considering these parameters, the device is **compliant** with this subparagraph. |
| 5.2 – Implement a means to manage reports for vulnerabilities  (Compliant) | This subparagraph includes information regarding reporting the vulnerabilities or potential issues and complies with additional regulations regarding the user awareness (for example letting the user know about the status of the problem). | The IoT device does have at least 2 ways of submitting issues that I have found myself. One of the ways, is to enter the **CMF Watch app**, and in the user profile, the user can send “feedback” which is referred to as problem reporting.  A screenshot of a black screen  Description automatically generated  Another way is by visiting <https://cmf.tech/en-be/pages/contact> and submitting the issue there.  Considering the regulation and my findings, I can say the device **complies** with this specific subparagraph |
| 5.3 – Keep software updated  (Partly compliant/Not compliant) | This subparagraph refers to the method the updates should arrive at the device itself. It mentions security concerns for the ways the updates are transmitted onto the device and enhances the security ways the device is being updated. | I could not test certain ways of the way the device secures its connection, or how it checks the authenticity of updates. However, all the updates only happen when the device is connected to the application on the smartphone and does an **automatic update once** at the first start and first pairing of the devices. All of the further updates, which are rather rare than it would be expected, are to be installed manually, by accessing the application, and then downloading the update onto the smartphone, and sending it over Bluetooth to the device.  A screenshot of a black screen  Description automatically generated  Taking into consideration the amount of information provided to me and the things I managed to see, I would rather say that the device is **not compliant** with this specific regulation, however it would need additional testing and documentation from the producer. |
| 5.4 – Securely store sensitive security parameters  (Not compliant) | This paragraph refers to information being stored on the device itself, tackling for example essential files and various other information that is present on the device. | The device in this case does not seem to have any important or crucial files stored on the on-board memory, apart from the software it uses itself (OS), and additional watch faces that can be uploaded via Bluetooth from the **CMF Watch app**. Any other information is not present in the documentation of the device, or any reviews available. Any other information like sleep data, monitoring data, is stored on the device and transmitted to the smartphone application once both are connected. However it is worth mentioning that the connection between smartphone and device is not always set, hence it is not being moved unless the user specifically triggers it.  Considering the findings, I would rather say the device is **not compliant** with this subparagraph. |
| 5.5 – Communicate securely | This subparagraph refers to usage of secure measures of communication with other devices, as well as ensuring secure ways of encrypting the data itself. | From my findings, I can say that the device supports secure pairing with companion app, and uses encrypted communication for data synchronization (which can be also favorable for **5.4**), which means the devices already partially complies with the requirements. However, the other parts regarding the cryptography regulations are not specified anywhere, hence full compliance can not be reached.  Considering the above information, I can state that the device is rather **not compliant** with this section. |
| 5.6 – Minimize exposed attack surfaces  (Not compliant) | This section refers to minimizing the possible threats that may arise in case of attack, or breach, or anything related. | Taking into consideration the various provisions specified, and the data that I have on hands, I can say that the device is supposed to be quite secure in terms of running processes and exposure onto the networks, as the device itself might only have processes that run once in a certain period of time, and when triggered by user. In terms of exposure, the device does get all the information like geolocation and updates and weather once connected to the smartphone, so in that case it minimizes the probability of some wrong things happening like an intrusion.  The functionality of the device is minimized and that provides it with additional surface for possible attacks.  Taking into consideration the things I have mentioned, I can say that the device is rather **not** **compliant**, especially considering the additional provisions. |
| 5.7 – Ensure software integrity  (Not compliant) | This section refers to the software present on the device itself like OS, and the various functions it has. | By checking the provisions related to this subparagraph, and by checking the available information, I can say that the device is rather **not compliant** as I cannot say if the device really uses secure boot for example, or if it has any other security functions. Something like unauthorized changes are not reported to the owner or device or whatsoever, hence in this particular section it becomes rather unsafe. |
| 5.8 – Ensure that personal data is secure  (Not compliant) | This section refers to the fact, that any data being transmitted should be protected with the best cryptography practices, and not only | Considering the provisions, I can say that the device would be compliant in case that the company producing the device would give out more information regarding the transmission of data and how it is being encrypted or secured, however for now the device is **not compliant** with this section. |
| 5.9 – Make systems resilient to outages  (Compliant) | This section refers to the device being able to operate on its own without connection to a network or anything of that kind. | In this case, since I am talking about a smart watch, the device itself can act as a separate device and does necessarily need connection to the smartphone for all its functions. However, it is worth mentioning that some functions will not be able to work properly without connecting to the smartphone, like yet again the weather functionality.  I can say that the device is **compliant** with this particular regulation. |
| 5.10 – Examine system telemetry data  (Compliant) | This is a section regarding collection of telemetry data, and how it can be used. | There is no information specified about the telemetry data being collected in any way, however I can not tell if there actually happens something in the background. The personal data, like user account in this case, is also handled by the company itself, so it should be compliant.  I think it will be easier to say that the device is rather **compliant,** because it does not have various functions of the device itself. |
| 5.11 – Make it easy for users to delete user data | This refers to the data being collected by the device, or any personal information being stored – it should be possible to delete it. | I have checked the various possibilities of data being stored on the device or smartphone, and can say that the device is rather **compliant** than not, due to the ability to get rid of data and reset the other information.  A screenshot of a device  Description automatically generated |
| 5.12 – Make installation and maintenance of devices easy  (Compliant) | This relates to the device being set up in an easy way and the user having clear instructions upon what to do. | While testing the device, and first setting that I had, I can say that the device is rather simple to understand, and it does not require much security tweaking to be usable by the user. All that is necessary is to link the device and then it is finished. Hence, I can say that the device is rather **compliant.** |
| 5.13 – Validate input data  (Not compliant) | This refers to the data is being processed or given to a device, which can be in various ways. | Trying to find data related to transmission and monitoring of data in the device, as well as processing of wrong data, does not give any probable and trustful results, as one of the provisions specifies that an API transferred data has to be validated, but due to the closed source of the software, I can not know (same as others) if the data is validated in any way. Hence, I will have to say it is **not compliant.** |

## Data protection provisions for consumer IoT

Taking into account the provisions specified in the 6th paragraph, it is also essential to specify information regarding personal data security and protection. In this particular case, the data that is being collected like telemetry data has not been specified, and the user is eventually asked to give consent towards privacy policy. That can mean that the company and the device itself try to be as compliant as possible, and as secure as possible, however I would say that for data protection it is rather **not compliant**.

## Summary

The regulation has provisions that specify various functions that the device is supposed to have, in order to be compliant with the whole section, however some of the mandatory requirements cannot be linked to this device, hence can be omitted or not put too much accent on.

***In conclusion, I will say that the device does not seem to be compliant with most of the provisions, which means that the device is rather unsecure, or there are a lot of things that are not talked about or shown to the public. This does not bring a lot of trust for the device itself and might make a user question if it is worth buying the device.***