National Test Institute for Cybersecurity

Radio Equipment Directive (RED)

Summary Report on the Cybersecurity of Connected Devices in the Context of the New RED Directive

Version	1.0
Date	22 May 2025
Classification	Public
Authors	Tobias Castagna, Patrik Fabian, Andreas Leisibach, Dilip Many, Raphael M. Reischuk, Fabio Zuber
Responsible	Tobias Castagna

Table of Contents

1 Management Summary

On 1 August 2025, the new requirements of the Radio Equipment Directive (RED) (2014/53/EU) will come into force in Switzerland. They require radio equipment to meet certain safety and health requirements and relate in particular to the cybersecurity of devices with an internet connection. The RED requirements apply to almost all devices with a radio interface. Numerous product categories are affected, including IoT devices, connected vehicles, Industry 4.0 applications, and smartphones. Devices newly placed on the market after the effective date of the RED must comply with the requirements. In the event of non-compliance, OFCOM may impose measures such as market bans.

The NTC analyzed a sample of connected devices. These are products from the following categories that are commonly sold in Swiss stores:

- Smartwatches for children
- Baby monitor cameras
- Alarm systems
- Smart plugs
- Wireless routers

The devices were tested according to a selected set of RED requirements chosen by the NTC to serve as examples. These include the following requirements that are central to the security and resilience of the devices tested:

- Authentication and access control (e.g. standard password requirements)
- Secure data communications (advanced encryption methods)
- Secure software updates (authenticity and integrity of updates)
- Protection against manipulation and unauthorized access (no insecure or undocumented interfaces)

A key finding of the NTC sample tests is that a significant number of the devices tested do not currently meet the new RED cybersecurity requirements. Specific examples illustrate the prevalence of these deficiencies: All the children's smartwatches and one alarm system tested had inadequate encryption when communicating with their respective manufacturers' cloud platforms. Several of the baby monitor cameras tested used insecure default passwords, and some models did not adequately protect the local radio transmission between the camera unit and the base station from eavesdropping. Most of the Wi-Fi routers and smart plugs tested also used no or inadequate encryption for communications. This potentially allows sensitive information such as Wi-Fi credentials or access keys, system settings and other data to be read by unauthorized parties.

The NTC sees an urgent need for action throughout the supply chain - from manufacturers to importers to retailers. To comply with the RED Directive, manufacturers are recommended to proactively implement the requirements, while importers and retailers are recommended to carefully select their suppliers and actively request evidence from their suppliers. Consumers can also contribute to their own security by shopping at established retailers in Switzerland, being cautious about direct imports, changing default passwords immediately and installing updates regularly.

2 Introduction

There is currently much discussion about the imminent introduction of new EU regulations such as the Cyber Resilience Act (CRA), which regulates the cybersecurity of products with digital elements, and the Network and Information Systems (NIS2) Directive, which defines cybersecurity requirements for operators of critical infrastructure. These directives are currently being adopted into national law in the various EU countries. Although Switzerland, as a non-EU country, is not directly affected, Swiss companies will have to comply with the requirements from the date of applicability in the EU if they operate in the EU.

In addition to CRA and NIS2, there is another, often less noticed directive: the Radio Equipment Directive (RED) (2014/53/EU). Unlike the aforementioned regulations, this directive has been transposed into Swiss law and therefore applies to almost all devices with a radio interface in Switzerland. Compliance is enforced by the Federal Office of Communications (OFCOM).

Originally introduced in 2014, RED has been continuously expanded and specified with legal acts, most recently in 2022, to include new cybersecurity requirements, primarily for devices with a radio interface that communicate over the Internet. The new requirements will go into effect on 1 August 2025 and will apply to devices newly placed on the market after that date. Numerous product categories will be affected, including IoT devices, childcare equipment, Industry 4.0 applications, and smartphones.

The broad scope of the RED is interesting: for example, the directive also regulates the EU-wide introduction of the universal USB-C charging connector for devices with wireless components, including smartphones, tablets, e-readers, digital cameras, laptops and headphones.

The National Test Institute for Cybersecurity NTC has analyzed a sample of connected devices with a radio interface regarding the new cybersecurity requirements of the Radio Equipment Directive (RED). The aim of the analysis is to assess the extent to which a selection of popular devices available in Switzerland already comply with the new cybersecurity requirements of the RED. It also intends to identify typical vulnerabilities and the need for action by manufacturers, importers, retailers and consumers.

The analysis shows that a large number of the devices tested do not comply with the new requirements. This applies in particular to basic security mechanisms such as secure authentication, encrypted communication, and update mechanisms. The results highlight the need for action at both the manufacturer and retailer level.

The main findings of the analysis are summarized in this report:

- The chapter **"Initial Situation and Approach"** describes the legal context of the RED and the approach followed in this analysis.
- The chapter **"Assessment Summary"** chapter provides an overview of the assessment results for the devices tested, without naming individual products or manufacturers, and summarizes the key findings of the analysis. Based on these findings, the chapter provides specific recommendations for manufacturers, importers, retailers and consumers.

3 Initial Situation and Approach

The Radio Equipment Directive (2014/53/EU) requires radio equipment to meet certain health and safety requirements. Specific new cybersecurity requirements, which particularly affect internet-connected devices, are laid down in Delegated Regulation (EU) 2022/30, which supplements the RED. These new requirements will become mandatory from August 1, 2025.

The "RED Cyber Requirements" as defined in Article 3.3 (d,e,f) of the RED Directive are further described and their test criteria defined in the harmonized standards EN 18031-1, EN 18031-2 and EN 18031-3. The standards are referenced as follows:

- **EN 18031-1:** Internet connected radio equipment
- **EN 18031-2:** radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
- **EN 18031-3:** Internet connected radio equipment processing virtual money or monetary value

The standards define many reasonable requirements, including secure access and authentication mechanisms, secure update and storage procedures, and logging and monitoring functions.

The NTC analyzed a sample of 20 connected devices. The sample consists of products frequently sold in the Swiss retail market in the following categories:

- Several smartwatches for children (category EN 18031-2)
- Several baby monitor cameras (category EN 18031-2)
- Several alarm systems (category EN 18031-1)
- Several smart plugs (category EN 18031-1)
- Several wireless routers (category EN 18031-1)

During the analysis, the devices were tested against a selection of RED requirements defined by the NTC. The RED requirements selected include various security mechanisms for Internet-connected radio equipment. These include the following requirements, which are central to ensuring the security and resilience of the tested devices:

Authentication and access control: The device must ensure that only authorized persons can access it. Default passwords such as "admin" or "1234" are not permitted.

- For example: A wireless router should require a strong, unique password when first set up or should not be delivered with easily guessable default credentials or access keys.

Secure data communications: Data transmissions must be protected by advanced encryption methods. This prevents data from being intercepted or manipulated during transmission.

- For example: A baby camera that transmits videos by radio must use eavesdropping-proof encryption to prevent unauthorized persons from monitoring the transmission

Secure software updates: The device should only install updates that have been

authenticated as coming from the manufacturer and verified that they have not been manipulated. Mechanisms are required to verify the authenticity and integrity of updates.

- For example: A children's smartwatch must ensure that only verified updates from the manufacturer can be installed to prevent malware from entering the device.

Protection against manipulation and unauthorized access: There must be no insecure or undocumented interfaces that attackers could exploit to take control of the device.

- For example: A smart plugs should not have any unsecured remote maintenance access enabled that could be used by an attacker to gain access without credentials or access keys.

To assess compliance, the devices were subjected to a review that included a selection of ten RED requirements. This selection represented approximately one-third of the complete RED requirements catalog. Even this reduced depth of assessment was sufficient to identify non- compliance in the majority of the devices. Even a single instance of non-compliance with one of the requirements will result in the entire device being deemed non-compliant and possibly having to be withdrawn from the market. It is therefore reasonable to assume that a full assessment of all RED requirements would have resulted in an even higher number of non-compliant devices.

This report deliberately does not name specific products or manufacturers as the focus is on the general market picture. The affected manufacturers have been notified directly by the NTC of the weaknesses identified.

4 Assessment Summary

The results of the sample conducted show that a significant number of the devices tested do not currently meet the new RED cybersecurity requirements. The most common weaknesses found include:

- **Use of insecure default credentials**: Numerous devices are delivered with easily guessable or commonly known default passwords (e.g., "admin," "1234"). There is often no mechanism to force users to change these insecure credentials the first time they use the device. This is a fundamental weakness because it is potentially very easy for attackers to gain control of the device.

- **Insufficient encryption of data communication:** In particular, the transmission of data between the device and the manufacturer's cloud services is often performed with inadequate or no encryption. This also potentially affects sensitive user data (e.g. video recordings, location data), which can be accessed or manipulated by third parties during transmission.

- **Inadequate security of update mechanisms:** The processes for installing software updates were seriously vulnerable on some devices. Fundamental checks to verify the integrity and authenticity of update files were missing. Such weaknesses potentially allow attackers to install manipulated or malicious software on the devices. In addition, some devices do not have update capabilities. This means that any vulnerabilities discovered on these devices cannot be fixed at a later date.

Specific examples illustrate the widespread nature of these weaknesses: all of the children's smartwatches and one alarm system tested had inadequate encryption when communicating with their respective manufacturers' cloud platforms. Several of the baby cameras tested used insecure default passwords; in addition, the local wireless transmission between the camera unit and the base station of some models was not sufficiently protected against eavesdropping. The majority of Wi-Fi routers and smart plugs tested also used no or inadequate encryption for communications. This means that sensitive information, such as Wi-Fi credentials or system settings, could potentially be read.

It should be emphasized that the selection of devices tested is not representative of the entire market. However, the NTC has deliberately selected current and popular products available on the Swiss market. The analysis shows that safety deficiencies are not only a problem with cheap products: Even more expensive devices from established manufacturers often fail to meet the new requirements.

Some of these deficiencies, such as the use of weak default passwords or the lack of a prompt to change the password, are in principle obvious to observant consumers. However, many critical vulnerabilities, such as encryption or update security, are not easily checked and require technical expertise.

With the stricter RED requirements coming into force on 1 August 2025 for all newly marketed devices with a radio interface, there is an urgent need for action for the entire supply chain - from manufacturers to importers and retailers. They are all responsible for ensuring that their products meet the legal safety requirements. The Federal Office of Communications (OFCOM) is responsible for market surveillance and monitoring compliance. In the event of non-compliance, it can order measures such as market bans.

To comply with the upcoming regulation, **manufacturers, importers and retailers** are advised to act proactively:

- **Proactively implement and verify security requirements:** Manufacturers should proactively and seamlessly implement the relevant cybersecurity requirements of the RED in their products. This requires security to be deeply integrated into the development process from the start ("security by design"). Full compliance with all required aspects must be actively verified through comprehensive testing and demonstrated for market approval.

- **Ensure and demonstrate compliance:** Manufacturers must ensure that their products comply with the requirements. Importers and retailers should actively request evidence from their suppliers that the Declaration of Conformity explicitly covers the new cybersecurity requirements (in accordance with Article 3.3 d, e, f of the RED).

- **Diligence in supplier selection:** Particularly for suppliers outside Switzerland and the EU, greater diligence is required. If necessary, conduct your own assessments or request detailed test reports that demonstrate compliance.

Consumers can also contribute to their security:

- **Buy from established retailers in Switzerland:** These retailers are required by law to ensure that the products they offer comply with Swiss regulations (including RED).

- **Be careful with direct imports:** The risk of receiving a non-compliant and potentially unsafe device is higher, especially with very low-cost offers from online platforms outside Switzerland and the EU. There is also a risk that such deliveries will be stopped by customs upon import, which can result in costs to the buyer.

- **Change default passwords immediately**: If a device offers the option, the default credentials or access keys should be changed to a strong, customized password the first time the device is used.

- **Install updates**: The software of connected devices should be kept up to date, provided the manufacturer offers updates.

Although the forthcoming regulation from August 2025 should lead to safer products in the long term, the current assessment results raise doubts as to whether it will be fully implemented on time. It remains to be seen how quickly the market will adapt to the new requirements. The National Test Institute for Cybersecurity NTC will continue to monitor developments and report on any weaknesses identified.