National Test Institute for Cybersecurity

PRESS RELEASE
Summary report on the cybersecurity of connected devices in the context of the new RED Directive

Many Connected Devices Fail to Comply with New Security Directive - Risking Market Bans from August 2025

Zug, 22 May 2025 – On 1 August 2025, stricter requirements of the Radio Equipment Directive (RED) will come into force in Switzerland. The RED sets new cybersecurity requirements for connected devices with a radio interface - such as smartwatches, Wi-Fi routers and baby cameras. A recent report by the National Test Institute for Cybersecurity NTC shows that a significant number of the products tested do not comply with the new requirements at this time. The NTC sees an urgent need for action throughout the supply chain.

The assessment examined devices that are widely available on the Swiss market, including children's smartwatches, baby cameras, alarm systems, Wi-Fi routers and smart socket adapters. As part of the analysis, the devices were tested for selected RED requirements. The focus was on aspects that are particularly relevant for the security and resilience of the devices: Authentication and access control, protected data communication, secure software updates and protection against manipulation and unauthorized access. The aim was to determine whether the tested products meet the cybersecurity requirements that will apply from August 2025.

Results of the sample assessment

The technical analysis shows widespread weaknesses such as insecure default passwords, missing or inadequate encryption during data transmission, and inadequate or missing mechanisms for software updates. These deficiencies were found not only in low-cost imported products, but also in devices from established brand manufacturers. The weaknesses identified show a significantly increased attack surface. Most alarming is the fact that some of these weaknesses can be exploited without in-depth technical knowledge. Devices with such deficiencies will not be considered RED-compliant and will not be allowed to be placed on the market after August 2025.

The new requirements will lead to safer products in the long run. However, the results of the assessment raise doubts on whether full and timely compliance will be achieved.

Recommendations for market participants

The NTC recommends that manufacturers implement the relevant cybersecurity requirements of the RED consistently and at an early stage. Cybersecurity must be embedded as an integral part of the development process, in line with the principle of "security by design". Importers and retailers are recommended to actively request evidence of compliance from their suppliers and to carefully select products. Consumers can also contribute to their own security by buying from established retailers in Switzerland, being careful with direct imports, changing default passwords immediately and installing regular updates.

To the report

Media contact:
Andreas W. Kaelin, Executive Management
+41 41 210 11 03, andreas.kaelin@ntc.swiss

About the National Test Institute for Cybersecurity NTC
The National Test Institute for Cybersecurity NTC contributes to Switzerland's security and digital sovereignty by proactively identifying critical vulnerabilities of digital products and risks of new digital technologies and supporting their mitigation. As a not-for-profit association based in Zug, the NTC observes the principles of independence and objectivity. On its own initiative, the NTC tests digital products and applications that are not adequately tested in Switzerland but are of great importance to the economy and society. The NTC also conducts cybersecurity tests on behalf of operators of critical infrastructures and public authorities.
https://en.ntc.swiss