National Test Institute for Cybersecurity

Cybersecurity of Peripheral Devices

Hidden risks in the office: Are wireless keyboards, headsets, and similar devices sufficiently secure for use in critical infrastructures?

Version	1.0
Date	26 February 2026
Classification	Public
Authors	Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Raphael M. Reischuk
Responsible	Tobias Castagna

Table of Contents

Acknowledgements

Special thanks go to all organizations and experts who supported this investigation, whether by providing test devices, sharing insights into the use of such devices in different environments, or contributing to the costs. Their outstanding commitment to cybersecurity made a decisive contribution to the success of this security analysis. These include:

- Federal Office for Cybersecurity (BACS)
- Federal Office of Communications (OFCOM)
- Federal Office for Customs and Border Security (FOCBS)
- Canton of Schwyz
- Digitec Galaxus
- Redguard AG
- Zuger Kantonalbank
- other Swiss financial institutions (not named for reasons of discretion)

1 Introduction

In today's working environment, IT security does not end at the network perimeter. While organizations invest heavily in protective measures such as firewalls and endpoint protection, a readily accessible attack surface in everyday operations is often underestimated: peripheral devices at the workplace.

A realistic scenario illustrates the risk: A confidential video conference at a critical infrastructure operator. The network is secured, the connection is end-to-end encrypted, the server is hardened, and the laptop is protected. However, the attacker targets something else. Using an antenna from a nearby parking area, they intercept the unencrypted radio traffic of a wireless tabletop microphone. Within seconds, the confidential conversation is being eavesdropped on – IT security has been undermined by an insecure peripheral device.

The underlying issue is a dangerous asymmetry: the cost of a professional security analysis capable of identifying such risks exceeds the purchase price of a webcam or keyboard many times over. In practice, IT departments therefore often rely on manufacturers' security claims.

To systematically assess the security level of peripheral devices widely used in Switzerland, the National Test Institute for Cybersecurity NTC conducted an extensive technical security analysis of approximately 30 devices over the course of one year. The selection deliberately focused on products from established manufacturers that are commonly used in Swiss organizations, particularly in critical infrastructures. Low-cost products of unknown origin were intentionally excluded.

In total, more than 60 findings of varying criticality were identified, including 13 high-severity findings and three classified at the highest criticality level.

The analysis shows that modern, well-designed peripheral devices — including wireless solutions — can generally achieve a high level of security. Crucially, however, security does not depend solely on individual components, but also on secure configuration choices and on clearly defined requirements governing the safe use of such devices. This includes organizational processes that ensure secure operation, such as the regular deployment of firmware updates and clarity regarding underlying assumptions.

Operators of critical infrastructures with elevated security requirements must in particular anticipate highly motivated and well-resourced attackers. Such adversaries may employ unconventional attack vectors and techniques that might be atypical in other contexts. For example, several tested wireless headsets and conference systems could be repurposed into covert listening devices with minimal effort. These and other risks are explained in this report and addressed through concrete measures and recommendations.

The detailed findings were disclosed confidentially to the affected manufacturers as part of a responsible disclosure process to enable quick remediation. Consequently, this public report deliberately refrains from disclosing technical details. Instead, it focuses on recurring risk patterns and the recommendations derived from them.

The analysis was conducted as part of a joint initiative by the National Test Institute for Cybersecurity NTC, with support from federal and cantonal authorities as well as organizations from the financial sector. To ensure the independence of the results, manufacturers of the tested devices were neither involved in the selection nor in the execution of the tests and were only contacted during the disclosure of vulnerabilities.

Five Recommended Measures for Improved Security

Based on the security analysis conducted, five key action areas can be identified to effectively reduce risks associated with the use of peripheral devices:

Standardization and Procurement via Trusted Channels
It is recommended to limit device diversity by defining a binding catalogue of approved and tested peripheral devices. Procurement should be carried out exclusively through trusted and authorized channels in order to reduce the risk of manipulated hardware and supply-chain attacks.

Integration into Lifecycle Management
Peripheral devices should not be treated merely as accessories, but as fully-fledged IT components. Security-relevant devices should therefore be recorded in asset management systems, and processes should be established to ensure, for example, the timely deployment of firmware updates and the rapid replacement of vulnerable or end-of-life hardware.

Network Segmentation
For network-capable systems such as conference solutions or IoT devices, operation within isolated network segments is recommended. This prevents such devices from being used as an entry point into the internal corporate network in the event of a compromise.

Physical Security and Awareness
Employees should be sensitized to the secure handling of peripheral devices. This includes the exclusive use of approved hardware in home office environments as well as awareness of the risks posed by unattended devices such as USB dongles or wireless headsets in public or semi-public spaces.

Wired Solutions in High-Security Areas
In environments with maximum protection requirements, wired peripheral devices should be preferred. Physical connections largely eliminate the risks associated with wireless signal transmission and significantly reduce the attack surface.

These measures summarize key recommendations. A detailed discussion of the technical background and specific mitigation strategies can be found in *Chapter 4: Recommendations* of this report.

2 Background and Methodology

Peripheral devices are far more than mere accessories: they form the physical interface between humans and computers, and sensitive information flows through them. For instance, passwords are entered via keyboards, and confidential conversations are transmitted through webcams and microphones. If such devices are insecure or manipulated, they can serve as entry points to bypass security mechanisms or be misused as covert surveillance tools. While workstations and smartphones benefit from increasingly robust security, peripheral devices often lack similar safeguards, posing a significant and unmonitored risk.

Two recent incidents show the relevance of this issue. In 2025, a series of vulnerabilities[1] were disclosed in widely used Bluetooth chips manufactured by Airoha. These flaws allow attackers to hijack Bluetooth connections and, for example, covertly listen in on confidential conversations. The affected chips are used in devices from brands such as Bose, Jabra, JBL, Teufel, Sony, and Marshall. The persistence of this risk became evident again in early 2026, when researchers uncovered severe flaws in the implementation of the "Google Fast Pair" protocol, known as "WhisperPair"[2]. These vulnerabilities allow attackers to take over headphones from manufacturers such as Google, Sony, Xiaomi, and OnePlus without any user interaction, enabling them to eavesdrop on surrounding conversations and track the user's location via the "Find My Device" network. Such incidents demonstrate that even products from well-known manufacturers are not immune to serious implementation errors.

Despite their critical role, vulnerability assessments of peripheral devices are rarely performed. There are several reasons for this:

- **Lack of risk awareness:** Peripheral devices such as keyboards are often perceived as simple, non-autonomous hardware. However, they now incorporate their own processors, firmware, and wireless interfaces, making them an integral part of the IT attack surface.
- **Economic barriers:** The cost of a professional security assessment often far exceeds the purchase price of such devices by several times, resulting in a significant economic imbalance.
- **Diffusion of responsibility:** The widespread use of peripheral devices frequently creates a false sense of security. Many organizations mistakenly assume that popular products, due to their high market penetration, have already been thoroughly tested by third parties and that any serious vulnerabilities would long since have been remediated.
- **Loss of control:** The rise of remote work and "bring your own device" (BYOD) practices has led to an unmanageable diversity of devices that often escapes centralized IT control.

For these reasons, the National Test Institute for Cybersecurity NTC conducted a comprehensive technical security assessment of approximately 30 commonly used peripheral devices. The selection included both wired and wireless products from established manufacturers such as Logitech, Yealink, Jabra, HP, Eizo, and Cherry. These devices are widely used in Swiss organizations, particularly in critical infrastructures. The

[1] CVE Details: *https://www.airoha.com/product-security-bulletin/2025*;
Analysis: *https://insinuator.net/2025/06/airoha-bluetooth-security-vulnerabilities*
[2] CVE: CVE-2025-36911; Analysis: *https://whisperpair.eu*

tested devices covered the following categories:

- **Keyboards and mice**
- **Headsets**
- **Webcams**
- **Docking stations**
- **Conference systems**

The testing activities and the subsequent responsible disclosure process with the manufacturers extended over a period of approximately one year. The analysis was carried out by four test experts from the National Test Institute for Cybersecurity NTC, in cooperation with several federal and cantonal authorities as well as organizations from the financial sector.

To ensure the independence of the results, the manufacturers of the evaluated devices were neither involved in the selection, procurement, nor execution of the tests. They were contacted only when the identified vulnerabilities were disclosed.

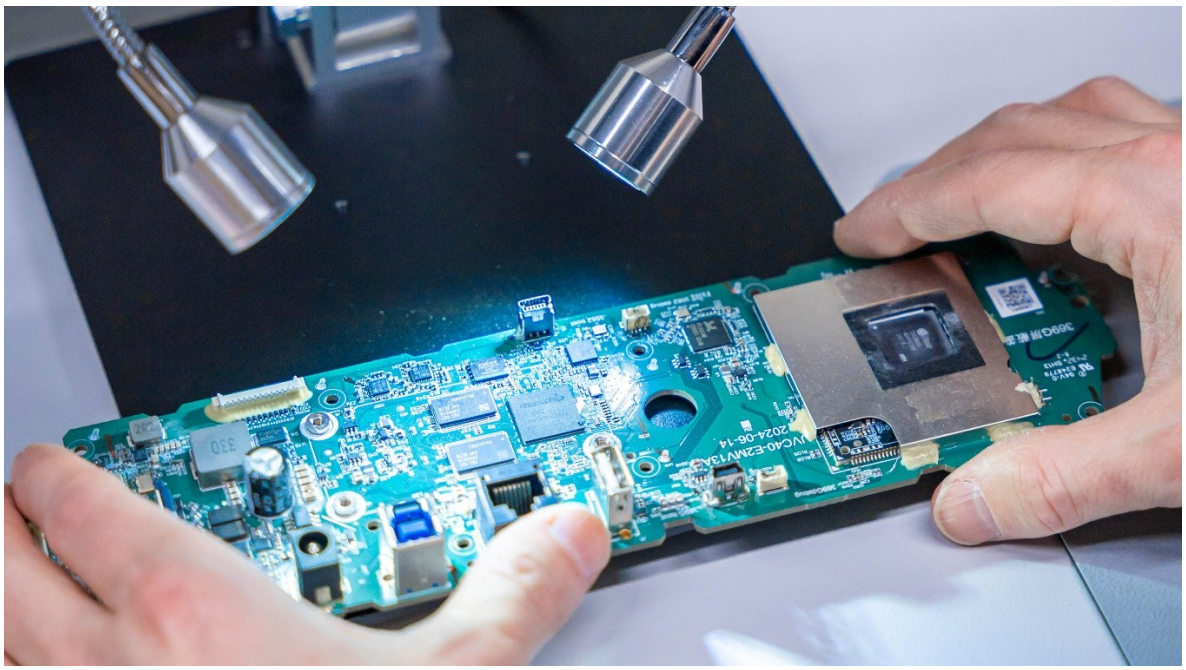

Figure 1: Visual inspection of peripheral device components at the laboratory of the National Test Institute for Cybersecurity NTC in Zug

To provide a sound assessment of the tested devices, the tests went far beyond mere functional checks. The analysis was conducted in multiple stages, employing methods such as:

- **Hardware Analysis:** The devices were physically opened to identify installed chips. The experts searched for open maintenance interfaces that could allow attackers to access the firmware, as well as for hidden or unexpected components that could indicate a supply chain attack.
- **Firmware Analysis:** The device software was extracted and examined using reverse engineering. The goal was, among other things, to detect hard-coded credentials, hidden backdoors, insecure encryption methods, or missing integrity checks that

would allow the installation of manipulated updates.

- **Wireless Analysis:** By sniffing and analyzing radio traffic, it was verified whether the communication between the peripheral device and its counterpart (dongle/PC) is encrypted and protected against manipulation.
- **Configuration and Interface Analysis:** The tests checked whether management interfaces, diagnostic ports, or additional communication protocols unnecessarily expanded the attack surface and whether the default settings adhered to the "security-by-default" principle.

3 Overall Assessment

Most products from well-known manufacturers exhibit an acceptable to good level of security, provided they are securely configured and their firmware is kept up to date. Nevertheless, more than 60 findings were identified during the tests, including 13 high-severity findings and three classified at the highest criticality level. The vulnerabilities were disclosed confidentially to the manufacturers as part of the responsible disclosure process and have largely been remediated by them. Many of the identified issues do not rely on entirely new attack methods, but rather on well-known attack techniques. Their exploitability in realistic scenarios underscores the need for action.

While classic input devices such as mice and keyboards are often solidly secured thanks to modern standards, risks increase significantly as soon as devices become more complex—such as conference systems and other IoT devices—or when outdated wireless technologies are used.

Representative examples of findings from the analysis include:

Critical Vulnerabilities in EZCast Pro II
The most severe finding concerns the wireless presentation system EZCast Pro II. Serious design flaws lead to critical vulnerabilities: hard-coded cryptographic keys allow access to the administrative interface, and Wi-Fi passwords can be derived from publicly observable identifiers. An attacker within wireless range can gain full control of the device and intercept screen content in unencrypted form. As the manufacturer did not remediate the vulnerabilities within the required timeframe, the case was escalated to the Federal Office for Cybersecurity (BACS), which issued a warning pursuant to Article 73c, paragraph 2 of the Information Security Act (ISA)[3].

False Sense of Security in Audio Encryption
One evaluated conference system uses encrypted wireless transmission for communication with its microphones. However, the encryption is implemented so weakly that an attacker can break it within seconds and eavesdrop on conversations.

Headsets as Covert Listening Devices
Several wireless headsets support simultaneous pairing with more than one device, such as smartphones or computers, as a desired feature. An attacker who briefly gains physical access to such a headset, for example during a moment of inattention on a train or during a visit to an office, can pair a second, attacker-controlled device. Subsequently, all conversations occurring near the headset can be covertly monitored, provided the headset is not actively in use (e.g., while in standby mode or in the charging dock).

This example illustrates that vulnerabilities do not always require sophisticated hacking techniques and do not necessarily demand advanced technical expertise. Since this behavior is an intended feature, there will be no traditional software patch. Risk mitigation must therefore be achieved through organizational measures.

“Shadow keyboards” and injection attacks
Similar to the headset scenario described above, an attacker can pair an additional, a “shadow keyboard” invisible to the user with the USB dongle connected to a workstation.

[3] *https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/cvd-cases/cvd-case-1-test.html*

Using this shadow keyboard, commands can be sent to the computer from distances of up to 100 meters, as if the attacker were physically present. This enables, for example, the injection of malicious commands or the installation and execution of malware.

Firmware manipulation
Some devices allow firmware to be installed without a valid digital signature. This enables attackers to deploy manipulated firmware and establish persistent access at the hardware level. Even reinstalling the operating system on the connected workstation or smartphone cannot remove such persistence. This class of vulnerability is also responsible for the so-called "*BadCam*[4]" attack, in which a webcam with manipulated firmware presents itself to the PC as a keyboard.

Insecure default settings
A recurring overarching issue is manufacturers' prioritization of convenience over security. Many devices are shipped with insecure default settings, such as default passwords or unnecessarily enabled interfaces, in order to simplify support and improve "plug-and-play" usability. This creates avoidable attack surfaces for attackers.

[4] *https://eclypsium.com/blog/badcam-now-weaponizing-linux-webcams/*

4 Recommendations

Securing peripheral devices requires a multi-layered approach that spans procurement, operation, and employee awareness. The following recommendations are intended to help organizations significantly reduce their attack surface with reasonable effort. While the implementation of these measures is generally recommended for all organizations to establish a solid baseline level of security, they are of particular urgency for organizations with elevated protection requirements.

4.1 Secure Procurement and Standardization

Security risks arising from insecure hardware can rarely be "patched" retroactively. They must be addressed at the procurement stage:

4.1.1 Outdated Protocols and Standards

While many manufacturers rely on established encryption mechanisms, implementation flaws continue to occur. Well-known attacks such as the interception of keystrokes (*KeySniffer*[5]) or the injection of keyboard and mouse inputs (*MouseJack*[6]) remain a threat, particularly for older and low-cost devices.

Measures:

- **Preference for standard protocols:** As a general rule, open and well-established standard protocols such as Bluetooth in their current versions should be preferred over proprietary, undocumented protocols. Standards are continuously reviewed by a broad community of security experts, reducing the likelihood of undiscovered vulnerabilities.
- **Security benefits of manufacturer dongles:** Organizations without in-depth wireless expertise should generally rely on manufacturer-provided dongles. These often offer a more robust security configuration than default endpoint settings, as critical parameters such as encryption are hardened at the factory level. Organizations with high security requirements and sufficient expertise should assess whether custom hardening of endpoints is more appropriate. While this provides greater control over all parameters, it requires deep technical knowledge and well-established processes for configuration and monitoring.

4.1.2 Supply-Chain Risks and Device Proliferation

The uncontrolled use of a wide variety of device models ("device sprawl") makes effective security management virtually impossible. In addition, there is a risk that devices may already be manipulated at the factory or during transport (supply-chain attacks).

Measures:

- **Standardization of device selection:** It is recommended to define a binding catalogue of tested and approved peripheral devices. Consistent enforcement of this catalogue—including in home office and mobile working scenarios—reduces complexity and prevents the use of potentially insecure no-name products.

[5] *https://keysniffer.net*
[6] *https://bastille.net/research/vulnerabilities-mousejack*

- **Selection of trusted sources:** Hardware should be procured exclusively through authorized channels of established manufacturers ("chain of trust"). This reduces the risk of manipulated devices to a certain extent.
- **Integration of information security into procurement processes:** Security requirements (e.g., signed firmware, guaranteed update support) should be defined as concrete and verifiable mandatory criteria in tenders and contracts. These requirements must be derived from the organization's own protection needs and must not be replaced by supplier-side risk assessments.

As a technical baseline, the standard ETSI EN 303 645 is suitable. It defines minimum security requirements for connected devices, whose compliance should be transparently demonstrated by suppliers (e.g., via a compliance matrix in accordance with Annex B).

4.1.3 Wireless Signals in High-Security Areas

In environments with maximum protection requirements, wireless interfaces often represent an avoidable expansion of the attack surface.

Measures:

- **Use of wired devices:** For workstations with high security requirements, wired peripheral devices such as keyboards, mice, and headsets should be mandated as the default. Physical connections largely eliminate the risks associated with wireless signal transmission.
- **Independent security assessments:** For particularly critical use cases, it is recommended to subject devices to regular independent security analyses. To leverage synergies from the analysis already conducted, the National Test Institute for Cybersecurity NTC can provide information on whether specific devices were included in the test scope.

4.2 Secure Operation and Configuration

Many of the identified vulnerabilities are technical in nature but only become critical as a result of organizational shortcomings.

4.2.1 Lifecycle Management and Firmware

During testing, numerous vulnerabilities were identified that have since been remediated by manufacturers. However, because peripheral devices are often not included in centralized IT patch management, updates either do not reach the devices at all or only with significant delay.

Measures:

- **Establish firmware update processes:** A process for the regular updating of peripheral device firmware should be established, analogous to the approach used for traditional IT components such as servers and laptops.
  - **Important note:** It is recommended to critically assess the permanent installation of manufacturer management software on end-user systems, as such software can itself increase the attack surface. Further details can be found in *Section 4.2.3 Manufacturer Software*.
- **Asset inventory:** Security-relevant peripheral devices should be recorded in asset management systems. Only devices that are inventoried can be reliably

decommissioned, securely disposed of, and properly disconnected at the end of their lifecycle.

4.2.2 System Hardening and Interface Control

Many devices are shipped with open interfaces and enabled convenience services ("plug-and-play"), which creates unnecessary attack surfaces.

Measures:

- **Disabling unused interfaces:** It is recommended to disable interfaces that are not strictly required for operation. This is particularly relevant for more complex devices such as conference systems with numerous connection options and applies to both physical ports (e.g., USB, Ethernet) and wireless interfaces (e.g., Wi-Fi, Bluetooth). This minimizes the attack surface.
- **Disabling unnecessary services:** Convenience features such as remote maintenance access, Telnet, and discovery protocols should be disabled on all devices unless they are strictly required for operation.

4.2.3 Manufacturer Software

Comprehensive manufacturer management tools often run permanently in the background and increase the attack surface on client systems.

Measure:

- **Minimalism in manufacturer software:** It is recommended to critically evaluate the necessity of installing manufacturer software on end-user systems. In many cases, basic operating system drivers are sufficient. If additional software is unavoidable, continuous background execution should be avoided. Firmware updates should instead be performed via dedicated update stations operated by IT support, eliminating the need for management software on end-user devices.

4.3 Secure Device Pairing

The pairing process represents a critical phase during which attackers may attempt to integrate their own devices into a trusted connection.

4.3.1 "Shadow Keyboards" and Covert Surveillance Devices

For some devices, attackers can connect to a victim's wireless dongle. This requires either brief physical access to the dongle or exploitation of a vulnerability in the pairing protocol. An invisible "shadow keyboard" can then inject malicious commands, or an unauthorized headset can function as a covert listening device.

Measures:

- **Awareness and training:** Employees should be trained not to leave mobile peripheral devices (e.g., USB dongles and headsets) unattended in public spaces.
- **Restriction of pairing capabilities**: Where technically feasible, dongles should be software-locked after initial pairing to prevent the subsequent addition of unauthorized devices. However, it must be acknowledged that this is often difficult to implement in practice.
- **Use in public environments:** In uncontrolled environments such as trains or cafés, it is

recommended to use only devices that technically prevent covert third-party pairing, for example through wired solutions.

4.4 Infrastructure and Conference Rooms

As complex multimedia devices were found to exhibit critical deficiencies particularly frequently during testing, the following additional recommendations are especially relevant for this category of devices.

4.4.1 Critical Vulnerabilities in IoT Devices

As demonstrated by the EZCast presentation system, vulnerabilities in conference systems can enable covert interception of screen content or full system compromise.

Measure:

- **Network separation:** Devices with their own network connectivity, such as IoT devices, video conferencing systems, and wireless presentation solutions, should be operated in isolated network segments. It must be ensured that these devices do not have direct access to the internal corporate network.

4.5 Regulatory Outlook

While the new cybersecurity requirements of the **Radio Equipment Directive (RED)** have been in force since August 2025 and obligate manufacturers to implement stronger cybersecurity measures, the forthcoming **Cyber Resilience Act (CRA)** will further expand these obligations. Among other requirements, it mandates security by design and compulsory security updates throughout the entire lifecycle of digital products.

However, it will take time for these regulations to fully permeate the market. Organizations should therefore not wait, but already today demand transparency and contractually binding commitments to cybersecurity from their suppliers.