

PRESS RELEASE

Summary Report on the Cybersecurity of Peripheral Devices

Underestimated Risk: How Keyboards, Headsets, and Other Peripherals Can Become Entry Points into Critical Systems

Zug, February 26, 2026 – A comprehensive technical analysis conducted by the National Test Institute for Cybersecurity NTC shows that peripheral devices used in the digital workplace are an often underestimated attack surface. Approximately 30 widely used keyboards, headsets, webcams, and conferencing systems from established manufacturers were tested in Switzerland—devices commonly found on office desks across the country. The NTC identified more than 60 vulnerabilities, including 13 high-severity and 3 critical vulnerabilities. The vulnerabilities were reported to the manufacturers and have largely been remediated.

A real-world scenario illustrates these risks: During a confidential video conference at a critical infrastructure operator, the network, server, and laptop are hardened and up to date, and the connection is end-to-end encrypted. An attack is nevertheless possible. Using an antenna in a nearby parking lot, an attacker intercepts the insufficiently secured wireless traffic of a tabletop microphone. Within seconds, they can listen in on the confidential conversation.

In this way, existing security measures can be bypassed through an insecure peripheral device. Peripheral devices constitute a critical interface through which sensitive information passes. Keyboards process passwords, while microphones and webcams transmit confidential conversations. A structural asymmetry emerges: The cost of professional security assessments often exceeds the purchase price of such devices by a wide margin. "In practice, peripheral devices are often treated as mere accessories and therefore are not systematically tested or consistently integrated into existing security frameworks," said Tobias Castagna, Head of Test Experts at the NTC.

Security Analysis Results and Key Risk Patterns

To systematically assess the security level of widely used peripheral devices in Switzerland, the NTC subjected approximately 30 wired and wireless devices to a comprehensive technical security analysis over the course of one year. The selection included products from established manufacturers such as Logitech, Yealink, Jabra, HP, Eizo, and Cherry, which are widely deployed in Switzerland, including in critical infrastructure environments.

In total, more than 60 vulnerabilities of varying severity were identified, including 13 high-severity and 3 rated critical. Several vulnerabilities can be exploited in realistic scenarios using known attack techniques. At the same time, the analysis shows that modern peripheral devices can achieve an acceptable security level when securely configured and operated with up-to-date firmware. However, risks increase with device complexity, particularly in conferencing systems or other IoT devices, as well as when outdated wireless technologies are used.

The identified vulnerabilities were reported to the affected manufacturers and were largely remediated promptly. In one case, however, a manufacturer did not respond. For a wireless presentation system, the NTC escalated the case to the National Cyber Security Centre (NCSC), which subsequently issued a public warning.

The public report deliberately refrains from disclosing technical details or product-specific vulnerabilities. Instead, it highlights pervasive risk patterns, including insecure default configurations, weaknesses in device pairing processes, insufficiently protected wireless communications, and deficiencies in firmware and lifecycle management. The analysis demonstrates that security in peripheral devices is not solely a product characteristic but depends significantly on configuration, operational practices, and clearly defined organizational requirements.

Recommendations for Risk Reduction

Based on the findings, the NTC formulates five general recommendations to reduce risks associated with the use of peripheral devices, particularly for operators of critical infrastructure and organizations with elevated security requirements:

- Standardization and secure procurement through trusted supply channels
- Inclusion of peripheral devices in IT lifecycle and asset management processes
- Network segmentation for network-enabled devices such as conferencing systems
- Preference for wired solutions in high-security environments
- Awareness training for personnel regarding physical and organizational risks

Implementing these measures enables organizations to significantly reduce their attack surface with reasonable effort.

The analysis was conducted as part of a joint initiative of the National Test Institute for Cybersecurity NTC, supported by federal and cantonal authorities as well as organizations from the financial sector. To ensure the independence of the results, the manufacturers of the tested devices were neither involved in the selection nor in the execution of the tests. They were contacted only in the course of confidential vulnerability disclosure to enable remediation.

[Summary Report](#)

Media contact:

Andreas W. Kaelin, Managing Director
+41 41 317 00 11, 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>