National Test Institute for Cybersecurity

PRESS RELEASE

NTC identifies severe vulnerabilities in hospital information systems and publishes recommendations

Zug, 23 January 2025 - The National Test Institute for Cybersecurity NTC has carried out a comprehensive technical security analysis of three of the most widely used hospital information systems (HIS) in several Swiss hospitals. The vendors have been informed and risk mitigation measures have been initiated. The published report identifies severe vulnerabilities and provides specific recommendations for improving cybersecurity in the healthcare sector.

Hospital Information Systems (HIS) are the backbone of modern hospitals. They control the flow of information, process sensitive patient data and ensure the smooth running of the hospital environment. The NTC's analysis has shown that the cybersecurity of these critical systems is often inadequate.

Findings of the analysis
Severe vulnerabilities were found in all of the systems tested. In total, more than 40 medium to critical vulnerabilities were identified. Three of these are of the highest criticality. Solutions based on outdated architectures are particularly vulnerable. The main issues include fundamental architectural problems, missing or inadequately implemented encryption, vulnerable surrounding systems, and insufficient separation between test and production environments.

Some of the vulnerabilities identified allowed full access to patient data and internal systems. While most of the relevant vulnerabilities have since been fixed or mitigated, some fundamental issues require a major redesign of the software architecture. This is a process that is likely to take several years, according to the vendors. In addition, the analysis uncovered several severe vulnerabilities in surrounding systems that were not part of the defined assessment scope, but were identified as incidental findings due to their conspicuousness.

The report deliberately refrains from providing details about the vulnerabilities. Instead, general information has been provided via the NTC Vulnerability Hub and impacted hospitals have been notified via the Cyber Security Hub (CSH) of the National Cyber Security Centre's (NCSC).

Recommendations for hospitals
The report contains eight key recommendations for the improvement of cybersecurity in Swiss hospitals. These include taking cybersecurity requirements into account when procuring IT and conducting regular vulnerability assessments for ongoing monitoring. In smaller hospitals in particular, cybersecurity responsibilities must be clearly defined and the necessary resources need to be made available. Closer networking between hospitals and access to the Cyber Security Hub (CSH) of the National Cyber Security Centre (NCSC) is also recommended.

The results underscore the need for regular security testing and clearly defined responsibilities. We would like to express our particular gratitude to the hospitals and organizations whose commitment to cybersecurity has been a key factor in the success of this security analysis.

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 and supporting their removal. As a not-for-profit association based in Zug, the NTC observes the principles of independence and objectivity. It conducts cybersecurity testing of networked infrastructures, devices and applications that are of great importance to society and the economy. https://en.ntc.swiss