National Test Institute for Cybersecurity

PRESS RELEASE
Summary Report on the Cybersecurity of Photovoltaic Systems

Systemically Important Photovoltaic Systems: NTC Presents Comprehensive Cybersecurity Analysis With Concrete Recommendations

Zug, 17 September 2026 – Photovoltaics has become systemically important to Switzerland's electricity supply. At the end of 2025, around 338,000 grid-connected photovoltaic systems were installed in Switzerland. That prompted the National Test Institute for Cybersecurity NTC to examine widely used systems on its own initiative. Seven inverters and four energy management systems in total underwent an in-depth analysis, which identified more than 50 findings, among them seven critical and six high. The findings were reported confidentially to the manufacturers. Most responded quickly, while work to fix the vulnerabilities is still under way for some products.

Results of the Security Analysis and Key Risk Patterns

To assess the security level of the photovoltaic technology in widespread use in Switzerland, the NTC put eleven products through a comprehensive technical security analysis over the course of a year: seven inverters and four energy management systems from eight manufacturers in total, including the market-leading providers.

In total, the assessments produced more than 50 findings, seven of them critical and a further six rated high. Five of the eleven products had at least one high or critical finding. On four products, the NTC gained complete control over the device — in some cases via remote code execution, in others through inadequately protected manufacturer maintenance access.

Four risk patterns recurred: deficiencies in authentication and access control, such as default passwords; insecure maintenance access with identical credentials across an entire device fleet; missing or weak encryption of communication over local interfaces; and interfaces that cannot be disabled. On almost every inverter tested, the local control interface made it possible — without any login — to change how much power the installation feeds into the grid, all the way down to zero.

Taken product by product, the security level is no worse than in other widely used connected devices the NTC has tested before. There was no evidence of deliberately built-in backdoors, and most manufacturers responded quickly once the vulnerabilities were reported. What sets solar installations apart from other connected devices is not the quality of the products but their role: collectively, they are systemically important to the power grid. Around midday on sunny days, they routinely cover more than half of the electricity being consumed at that moment.

What makes a finding matter for the grid is not its severity alone, but its reach. A single solar installation on a residential or commercial roof counts for nothing on the grid: if it fails or is manipulated, it makes no difference to the system as a whole. The risk comes from the fact that many of these installations are connected to their manufacturers' clouds and receive firmware updates, among other things, through that channel. Six of the findings act through such a central point on an entire fleet of devices, and therefore potentially on thousands of installations at once. "It is not the severity of a vulnerability alone that makes it dangerous, but its reach," says Tobias Castagna, Head of Test Experts at the NTC. "With photovoltaic systems, a single finding in a central component can affect thousands of installations at once — which is why targeted but workable countermeasures are needed here."

National Test Institute for Cybersecurity

Recommendations for Minimizing Risk

The NTC has already reported the findings to the manufacturers concerned ahead of publication. Many responded immediately and have already closed the gaps.

Based on what this analysis found, the NTC has set out recommendations for five audiences on measures to reduce cyber risks in photovoltaic systems:

- **Operators of small-scale installations:** choose an established provider, have it confirmed at handover that individual passwords have been set, and agree contractually who is responsible for updates
- **Operators of larger installations:** inventory interfaces and remote access, separate the installation from the rest of the network, and include security requirements in tenders
- **Installation companies:** set individual credentials for every installation, make sure it is not directly reachable from the internet, separate it from the rest of the network, and document the handover
- **Manufacturers:** treat security as a design principle — individual credentials, signed firmware updates, maintenance access that is time-limited and revocable, and a factory-set lock on grid-relevant remote control that can be released only on site
- **Policymakers and authorities:** minimum requirements for placing inverters and energy management systems on the market, security requirements as a condition of grid connection, and a designated responsibility for the risk that arises from small-scale installations taken together

There is no simple, complete solution. Every approach has advantages and disadvantages, and these recommendations do not cover the full range of possible measures. But every measure listed here improves cybersecurity once it is put in place.

The NTC initiated the analysis and provided the test team along with a substantial share of the funding. SwissEnergy provided financial support. Several organizations, most of them from the energy sector, supplied test devices and contributed to the costs.

The NTC thanks all the organizations involved, and SwissEnergy, for their support. To ensure the independence of the results, neither the manufacturers nor the supporting organizations had any influence on the selection of products, the scope of testing, or the results. The manufacturers were contacted only as part of the confidential disclosure process, so that they could remediate the vulnerabilities.

Photovoltaics 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