National Test Institutet for Cybersecurity

Press release

Security vulnerabilities in public electric mobility charging infrastructure identified and rectified

Zug, November 15, 2023 – In its latest project, the National Test Institute for Cybersecurity NTC conducted a comprehensive security analysis of Switzerland's charging infrastructure for electric mobility. Serious security vulnerabilities were identified at around 30 organizations. These were reported to the manufacturers, who then rectified them. The findings were also used to create general recommendations for the industry.

The National Test Institute for Cybersecurity NTC took the opportunity to subject the rapidly growing public charging infrastructure for electric mobility to a security analysis while it was still being developed. Due to the driving force of innovative startups, the number of public charging points is growing fast. Cybersecurity is often neglected in favor of a rapid market launch, something which jeopardizes sustainable development and stable operation.

In the period from May to August 2023, Internet-accessible systems from around 50 different manufacturers were tested, including seven mobile apps, the firmware of 11 charging stations and central backend applications from 23 charging station operators. The results of the tests highlight that the security situation in the area of public charging infrastructure for electric mobility in Switzerland is in need of improvement.

The final report summarizes the findings and makes them available to the public. The report is aimed in particular at manufacturers and operators of charging infrastructure and, in addition to risks, presents five general recommendations for the industry.

One of the most striking risks is the widespread use of an obsolete and non-secure version of the OCPP communication protocol within the industry. Manufacturers should only use the latest version of the protocol, as it has been upgraded with key security features.

In addition, all companies lacked the vulnerability disclosure policies recommended by the NCSC, which provide for the standardized publication of the contact details of a vulnerability reporting office, among other things. This would facilitate reporting by ethical hackers, as in practice it is otherwise difficult to contact the affected companies to report vulnerabilities.

The NTC has informed around 30 manufacturers and operators of vulnerabilities. The tests and the final report are therefore only part of the actual work, as notifying and advising the affected organizations is an important, time-consuming and invisible part of the overall effort required by the project.

The NTC's aim with this project is to point out potential vulnerabilities in this early expansion phase of charging infrastructure so that these can be addressed as early as possible and a robust and effective charging infrastructure can be built and operated in Switzerland.

LINK 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 NTC is the national competence center for independent testing of the cybersecurity and trustworthiness of digital products and networked infrastructures. The testing laboratory in the canton of Zug works closely with research institutions, private cybersecurity companies and international experts. The NTC was established in December 2020. https://en.ntc.swiss/