Institut national de test pour la cybersécurité

Communiqué de presse

Des failles de sécurité identifiées et comblées dans l'infrastructure de recharge publique pour l'électromobilité

Zoug, le 15 novembre 2023 – Dans le cadre de son dernier projet d'initiative, l'Institut national de test pour la cybersécurité NTC a soumis l'infrastructure de recharge suisse pour l'électromobilité à une analyse de sécurité approfondie. Des failles de sécurité majeures ont été constatées dans une trentaine d'organisations. Les vulnérabilités ont été signalées aux fabricants et supprimées par ces derniers. En outre, des recommandations générales sur les mesures à prendre ont été formulées pour le secteur.

C'est ainsi que l'Institut national de test pour la cybersécurité NTC a soumis l'infrastructure de recharge publique pour l'électromobilité, laquelle connaît une croissance fulgurante, à une analyse de sécurité dès sa mise en place. Face à la force motrice des start-ups innovantes, le nombre de points de recharge publics augmente rapidement. La cybersécurité est souvent négligée au profit d'un rapide lancement sur le marché, compromettant ainsi un développement durable et un fonctionnement stable.

Entre mai et août 2023, les systèmes d'une cinquantaine de fabricants différents, accessibles via Internet, ont été testés, dont sept applications mobiles, le firmware de onze bornes de recharge et des applications back-end centrales de 23 opérateurs de bornes de recharge. Les résultats des tests mettent en évidence des améliorations à apporter à la sécurité de l'infrastructure de recharge publique pour l'électromobilité en Suisse.

Le rapport final résume les conclusions et les rend accessibles au public. Ce rapport s'adresse en particulier aux fabricants et aux opérateurs d'infrastructures de recharge et présente, outre les risques, cinq recommandations générales sur les mesures à prendre pour le secteur.

L'un des risques les plus flagrants est l'utilisation d'une version obsolète et peu fiable du protocole de communication OCPP, très répandue dans le secteur. Les fabricants ne devraient utiliser que la dernière version du protocole, car elle est dotée de caractéristiques de sécurité importantes.

De plus, aucune entreprise ne disposait de Politique de divulgation des vulnérabilités, recommandées par le NCSC et prévoyant notamment la publication standardisée des coordonnées d'un service de signalement des vulnérabilités. Cette politique faciliterait le signalement par les hackers éthiques. Sans elle, il est difficile, dans la pratique, de contacter les entreprises concernées pour signaler les vulnérabilités.

Le NTC a informé une trentaine de fabricants et d'opérateurs des vulnérabilités constatées. Les tests et le rapport final ne représentent ainsi qu'une partie du travail proprement dit, la communication et le conseil aux organisations concernées constituant des tâches importantes, fastidieuses et imperceptibles pour le public dans le cadre du projet.

Avec ce projet d'initiative, le NTC a pour objectif d'attirer l'attention sur d'éventuelles vulnérabilités à ce stade précoce du développement de l'infrastructure de recharge afin de pouvoir y remédier le plus tôt possible et de mettre en place et exploiter une infrastructure de recharge solide et performante pour la Suisse.

LIEN VERS LE RAPPORT (Anglais)

Contact presse:
Andreas W. Kaelin, Directeur général
+41 41 210 11 03, andreas.kaelin@ntc.swiss

À propos de l'Institut national de test pour la cybersécurité NTC
Le NTC est le centre de compétences national pour le contrôle indépendant de la cybersécurité et de la fiabilité des produits numériques et des infrastructures en réseau. Le laboratoire de test et de contrôle du canton de Zoug travaille en étroite collaboration avec des instituts de recherche, des entreprises privées spécialisées en cybersécurité et des experts internationaux. Le NTC existe depuis décembre 2020.
https://fr.ntc.swiss