Institut national de test pour la cybersécurité

COMMUNIQUÉ DE PRESSE
Rapport de synthèse sur la cybersécurité des installations photovoltaïques

Installations photovoltaïques d'importance systémique: le NTC présente une analyse approfondie de la cybersécurité avec des recommandations concrètes

Zoug, 17 septembre 2026 – Les installations photovoltaïques sont devenues d'importance systémique pour l'approvisionnement en électricité de la Suisse. Fin 2025, la Suisse comptait environ 338 000 installations photovoltaïques raccordées au réseau. Dans ce contexte, l'Institut national de test pour la cybersécurité NTC a testé de sa propre initiative des systèmes très répandus en Suisse. Au total, sept onduleurs et quatre systèmes de gestion de l'énergie ont été soumis à une analyse approfondie. Plus de 50 constats ont ainsi pu être identifiés, dont sept critiques et six élevés. Les constats ont été signalés de manière confidentielle aux fabricants. La plupart ont réagi rapidement, tandis que pour certains produits l'élimination des vulnérabilités est encore en cours.

Résultats de l'analyse de sécurité et principaux schémas de risque

Pour évaluer le niveau de sécurité de la technique photovoltaïque répandue en Suisse, le NTC a soumis onze produits, au cours d'une année, à une analyse technique de sécurité approfondie: sept onduleurs et quatre systèmes de gestion de l'énergie de huit fabricants au total, dont les fournisseurs qui déterminent le marché.

Au total, les tests ont donné plus de 50 constats, dont sept critiques et six autres élevés. Cinq des onze produits présentaient au moins un constat élevé ou critique. Sur quatre produits, le NTC a obtenu le contrôle complet de l'appareil – en partie par du code injecté, en partie par un accès de maintenance du fabricant insuffisamment protégé.

Quatre schémas de risque sont apparus de manière récurrente: des défauts d'authentification et de contrôle d'accès, par exemple des mots de passe par défaut; des accès de maintenance non sécurisés avec des identifiants identiques pour tout le parc d'appareils; l'absence ou la faiblesse du chiffrement des communications via les interfaces locales; ainsi que des interfaces qui ne peuvent pas être désactivées. Sur presque tous les onduleurs testés, il était possible de modifier par l'interface de commande locale, sans authentification, la puissance que l'installation injecte, jusqu'à zéro.

Le niveau de sécurité des différents produits n'est pas moins bon que celui d'autres appareils connectés très répandus que le NTC a déjà testés. Aucun indice de portes dérobées intentionnellement intégrées n'a été trouvé, et la plupart des fabricants ont réagi rapidement aux vulnérabilités annoncées. Ce qui distingue les installations solaires d'autres appareils connectés n'est pas la qualité des produits, mais leur rôle: dans leur ensemble, elles sont d'importance systémique pour le réseau électrique. Les jours ensoleillés, à la mi-journée, elles couvrent régulièrement plus de la moitié de la consommation instantanée d'électricité.

Ce qui rend un constat pertinent pour le réseau, ce n'est pas sa seule gravité, mais sa portée. L'installation solaire individuelle sur le toit d'un bâtiment d'habitation ou commercial reste sans importance pour le réseau électrique: qu'elle tombe en panne ou qu'elle soit manipulée ne change rien au système dans son ensemble. Ce qui devient un risque, c'est que bon nombre de ces installations sont raccordées aux clouds des fabricants et reçoivent par cette voie, par exemple, les mises à jour du micrologiciel. Six des constats agissent, via une telle instance centrale, sur tout un parc d'appareils et donc potentiellement sur des milliers d'installations à la fois. «Ce n'est pas la seule gravité d'une vulnérabilité qui la rend dangereuse, mais sa portée», déclare Tobias Castagna, responsable des experts en tests au NTC. «Dans les installations photovoltaïques, un seul constat dans un composant central peut concerner des milliers d'installations à la fois – c'est pourquoi il faut ici des contre-mesures ciblées, mais réalisables.»

Recommandations pour réduire les risques

Le NTC a communiqué les constats aux fabricants concernés avant même la publication du rapport. Beaucoup ont réagi sans délai et ont déjà comblé les failles.

Sur la base des enseignements tirés de cette étude, le NTC a formulé, pour cinq groupes de destinataires, des recommandations de mesures visant à réduire les cyberrisques liés aux installations photovoltaïques:

- **Exploitantes et exploitants de petites installations:** choix d'un fournisseur établi, confirmation de mots de passe individuels lors de la remise et clarification contractuelle de la responsabilité pour les mises à jour
- **Exploitants d'installations plus grandes:** inventaire des interfaces et des accès à distance, séparation du reste du réseau ainsi qu'exigences de sécurité dans les appels d'offres
- **Entreprises d'installation:** identifiants individuels pour chaque installation, aucune accessibilité directe depuis Internet, séparation du reste du réseau et une remise documentée
- **Fabricants:** la sécurité comme principe de conception – identifiants individuels, mises à jour du micrologiciel signées, accès de maintenance limités dans le temps et révocables ainsi qu'un verrouillage en usine de la commande à distance des fonctions pertinentes pour le réseau, qui ne peut être levé que sur place
- **Monde politique et autorités:** exigences minimales pour la mise sur le marché d'onduleurs et de systèmes de gestion de l'énergie, exigences de sécurité comme condition du raccordement au réseau ainsi qu'une entité clairement désignée comme responsable du risque né de la somme des petites installations

Il n'existe pas de solution simple et complète; toutes les approches ont des avantages et des inconvénients, et ces recommandations ne couvrent pas l'ensemble des mesures possibles. Mais chacune des mesures citées ici, dès lors qu'elle est mise en œuvre, accroît la cybersécurité.

L'étude a été menée à l'initiative de l'Institut national de test pour la cybersécurité NTC, qui a également fourni l'équipe de test et une part substantielle des moyens financiers. L'étude a bénéficié du soutien financier de SuisseEnergie. Plusieurs organisations, majoritairement du secteur de l'énergie, ont mis à disposition des appareils de test et participé aux coûts.

Le NTC remercie toutes les organisations impliquées ainsi que SuisseEnergie pour leur soutien. Afin de garantir l'indépendance des résultats, ni les fabricants ni les organisations de soutien n'ont eu d'influence sur la sélection, l'étendue des tests ou les résultats; les fabricants n'ont été contactés que dans le cadre du signalement confidentiel en vue de l'élimination des vulnérabilités.

Rapport de synthèse photovoltaïque

Contact médias:
Andreas W. Kaelin, directeur
+41 41 317 00 11, andreas.kaelin@ntc.swiss

À propos de l'Institut national de test pour la cybersécurité NTC
L'Institut national de test pour la cybersécurité NTC contribue à la sécurité et à la souveraineté numérique de la Suisse en identifiant de manière anticipée les vulnérabilités critiques des produits numériques et les risques des nouvelles technologies numériques, et en soutenant leur atténuation. Association à but non lucratif d'intérêt public dont le siège est à Zoug, le NTC suit les principes d'indépendance et d'objectivité. De sa propre initiative, le NTC teste des produits et applications numériques qui ne sont pas suffisamment testés en Suisse mais qui revêtent une grande importance pour l'économie et la société. Le NTC réalise également des analyses de cybersécurité sur mandat d'exploitants d'infrastructures critiques et d'autorités. https://fr.ntc.swiss