Communiqué de presse

Flare alerte sur la menace croissante de cybersécurité pesant sur l'infrastructure de recharge des véhicules électriques

Sa dernière étude révèle que sur 1000 terminaux de recharge analysés et présents sur Internet, 72 % ne disposent pas de chiffrement du trafic

Paris, le 18 août 2026 – Dans un contexte où le marché automobile européen accélère sa transition vers l'électrique (1,22 million de voitures électriques ont été immatriculées dans l'Union européenne au 1er semestre 2026[1]) le besoin en infrastructures de recharge devient essentiel. Mais leur cybersécurité ne semble pas progresser au même rythme. Une nouvelle étude de Flare a analysé 1 000 bornes de recharge pour véhicules électriques accessibles via Internet dans 56 pays. 72 % acceptaient des connexions sans chiffrement, autrement dit, le protocole transportant les jetons d'authentification, les commandes de session et l'accès aux systèmes de paiement et aux serveurs s'exécutaient en clair sur la plupart des bornes observées

L'Europe concentre une part importante des infrastructures exposées

L'étude de Flare souligne que l'exposition des bornes est principalement concentrée en Europe. Ainsi l'Allemagne est en tête avec 234 bornes, devant les États-Unis (148). La France arrive en troisième position avec 63 bornes, devant la Chine (46). Ces chiffres ne correspondent toutefois pas au nombre de bornes physiques vulnérables dans chaque pays car un même système de gestion peut piloter plusieurs bornes et la géolocalisation correspond à l'adresse IP du terminal observé. Flare souligne donc qu'il s'agit d'une mesure de la surface de gestion exposée, et non d'un recensement des parcs nationaux de bornes.

Un protocole historique encore largement utilisé

Au cœur du problème se trouve le standard OCPP (Open Charge Point Protocol), qui permet aux bornes connectées de communiquer avec leurs systèmes de gestion. Sa version OCPP 1.6,

[1] Source : https://www.acea.auto/pc-registrations/new-car-registrations-5-7-in-h1-2026-battery-electric-20-7-market-share

lancée en 2015 est toujours la plus utilisée bien qu'elle ne comporte aucun chiffrement intégré. Le trafic entre une borne et son système backend peut donc circuler en clair si l'opérateur ne met pas en place de protection supplémentaire, comme un VPN ou une liaison cellulaire isolée.
Les versions OCPP 2.0.1 et 2.1 ont depuis introduit une sécurité reposant sur des certificats, mais Flare ne les a que rarement identifiées parmi les 1 000 terminaux analysés. Le renouvellement du matériel prend du temps et la rétrocompatibilité n'est pas systématiquement garantie.
L'étude met également en évidence un phénomène de concentration technologique : trois plateformes représentent à elles seules environ un tiers des terminaux observés. Le système de gestion open source SteVe compte 216 endpoints, dont 167 sans transport chiffré ; une deuxième pile logicielle comprend 66 endpoints, tous sans TLS, et une troisième plateforme en comprend 58, là encore sans connexion chiffrée.
Cette concentration augmente le risque : une configuration ou une faiblesse reproduite par défaut peut potentiellement se retrouver sur des centaines de déploiements.

Des incidents qui montrent que le risque n'est plus théorique
Les conséquences potentielles ne se limitent pas à l'indisponibilité d'une borne. Les incidents recensés ces dernières années couvrent déjà plusieurs niveaux de risque : exposition de données personnelles, compromission des systèmes de paiement, prise de contrôle d'équipements et attaque de la chaîne d'approvisionnement. En novembre 2024, environ 116 000 enregistrements provenant d'une application de recharge utilisée par des opérateurs dans huit pays ont ainsi été retrouvés sur un forum du darkweb. Ils comprenaient notamment des noms, des adresses, des identifiants de véhicules, des clés et jetons d'authentification ainsi que la géolocalisation précise de stations.

Pour Flare, les mesures techniques nécessaires sont connues : généraliser le chiffrement TLS, migrer vers OCPP 2.0.1 ou une version ultérieure, retirer les interfaces de gestion de l'Internet public, segmenter les bornes des systèmes critiques et surveiller en continu leur exposition externe.

À propos de Flare
Flare est une plateforme adoptée par des centaines d'entreprises dans le monde, elle aide à prévenir les prises de contrôle de comptes, les attaques par ransomware et les fuites de données résultant de la compromission d'identités humaines ou machines. Leader du Cyber Threat Intelligence centré sur les identités, Flare permet aux organisations d'identifier les expositions à haut risque affectant les identités en s'appuyant sur la plus importante base de stealer logs, de forums cybercriminels et de données d'identités compromises du secteur. Pour plus d'informations, rendez-vous sur le site web ou testez un essai gratuit pour découvrir la plateforme par vous-même. Rejoignez notre communauté Discord et explorez la Flare Academy pour rester informé des dernières actualités en matière de threat intelligence.