SYNACKTIV

Communiqué de Presse

Cybermenace sur les véhicules électriques, des failles critiques exposent un risque massif

Des vulnérabilités de sécurité mettent en péril l'ensemble de l'écosystème des voitures connectées et des infrastructures de recharge.

Paris, le 5 février 2025 – Les chercheurs de Synacktiv, experts en cybersécurité offensive et en recherche de vulnérabilités, ont identifié et exploité plusieurs failles critiques au sein de l'écosystème des véhicules électriques et connectés. Ils mettent en lumière des vulnérabilités inquiétantes pour l'industrie automobile et les infrastructures de recharge. Ces découvertes révèlent des surfaces d'attaque jusqu'ici sous-estimées, qui pourraient être exploitées par des cybercriminels pour compromettre la sécurité des utilisateurs et perturber l'approvisionnement en énergie.

Des infrastructures de recharge vulnérables

Les hackers éthiques de Synacktiv ont découvert des failles exploitables dans plusieurs dispositifs clés de recharge de véhicules électriques, notamment :

- **Le Tesla Energy Wall Connector**, qui présente une vulnérabilité de dépassement de tampon (buffer overflow) via le câble de charge, ouvrant la porte à des manipulations malveillantes.
- **Les bornes Autel MaxiCharger et ChargePoint Home Flex**, dont le protocole de communication entre le véhicule et le réseau électrique peut être détourné, mettant en péril l'intégrité des transactions énergétiques.
- **Des systèmes d'infodivertissement embarqués (IVI)** ont également été compromis, révélant un risque de prise de contrôle à distance des fonctionnalités critiques du véhicule.

Ces vulnérabilités montrent que les infrastructures de recharge, souvent considérées comme des équipements secondaires, constituent en réalité des points d'entrée stratégiques pour d'éventuelles cyberattaques.

Un risque pour l'ensemble de l'écosystème automobile

L'exploitation de ces failles pourrait avoir des conséquences graves, telles que :

- **intrusions réseau** : Les attaquants pourraient utiliser ces vulnérabilités pour s'infiltrer dans les réseaux internes des opérateurs de recharge et des constructeurs automobiles.
- **manipulation des flux d'énergie** : Une prise de contrôle des systèmes de charge pourrait engendrer des perturbations sur la gestion de l'électricité, altérant la facturation et la distribution d'énergie.
- **interruption des services** : L'exploitation de ces failles pourrait rendre certaines bornes de recharge inopérantes, impactant directement les utilisateurs et la continuité du service.

L'évolution des technologies, notamment l'intelligence artificielle, permet aux cybercriminels d'automatiser leurs attaques, rendant les intrusions plus rapides et complexes à détecter. Parallèlement, les stratégies de défense doivent s'adapter en temps réel en intégrant des protocoles de communication sécurisés et des mécanismes de détection avancés.

Un appel à la collaboration entre industriels et experts en cybersécurité

Face à ces menaces croissantes, Synacktiv appelle l'ensemble des acteurs du secteur – constructeurs automobiles, fournisseurs d'infrastructures de recharge, et spécialistes en cybersécurité – à intensifier leur collaboration. La mise en place de tests de sécurité réguliers, l'audit des systèmes et l'intégration de la cybersécurité dès la conception des équipements sont désormais indispensables pour sécuriser l'écosystème des véhicules électriques et connectés.

Ces découvertes ont été mises en lumière à l'occasion du concours international Pwn2Own Automotive 2025 qui vient de se dérouler à Tokyo, où l'équipe de chercheurs de Synacktiv s'est à nouveau illustrée en remportant la deuxième place. C'est la quatrième fois que Synacktiv se disngue et démontre un savoir-faire et une expertise pointue dans sa capacité à identifier des vulnérabilités critiques sur des technologies de pointe, notamment en compromettant des systèmes Tesla. Les fabricants concernés travaillent activement à la correction des failles identifiées[1]. Cette alerte rappelle l'urgence d'une approche proactive face aux menaces émergentes du secteur automobile.

1. Dans le cadre du concours Pwn2Own Automotive, les constructeurs disposent généralement de 90 jours pour corriger les vulnérabilités découvertes avant que les détails techniques soient rendus publics. Ce délai leur permet de développer et déployer des correctifs de sécurité afin de protéger les utilisateurs contre d'éventuelles exploitations malveillantes. Il peut toutefois varier en fonction des politiques de Trend Micro's Zero Day Initiative, qui organise l'événement, ainsi que de la criticité des failles identifiées.

A propos de Synacktiv

Entreprise française spécialisée en cybersécurité offensive, fondée en 2012 par deux experts en sécurité, ses principaux domaines d'expertise sont les tests d'intrusions, les audits de sécurité, la rétro-ingénierie, la recherche de vulnérabilités et la réponse à incidents.

Synacktiv participe à des projets sensibles de renommée mondiale. Elle développe de nombreux outils de sécurité offensifs dans le cadre de ses activités.

Synacktiv est agréée PASSI RGS et LPM (Prestataire d'Audit de la Sécurité des Systèmes d'Information) & CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) par l'ANSSI. Labellisée Cybersecurity Made In Europe par l'Alliance pour la Confiance Numérique (ACN), organisme certificateur autorisé par l'Autorité nationale des jeux (ANJ).

L'entreprise compte plus de 400 clients et emploie actuellement une équipe de plus de 180 experts en cybersécurité. Elle opère principalement depuis ses bureaux de Paris, Bordeaux, Toulouse, Lyon, Lille et Rennes. Les équipes interviennent en France, en Europe et à l'international.

A une échelle nationale ou internationale, l'implication de Synacktiv au sein de la communauté cyber se traduit par la participation à de nombreux évènements (conférences, challenges, CTF) ainsi que la publication régulière d'alertes de sécurité ou d'articles.

Pour en savoir plus www.synacktiv.com

A propos de ZDI (Zero Day Initiative)

Zero Day Initiative (ZDI) organise le concours de piratage Pwn2Own, qui a lieu trois fois par an, au cours duquel des équipes de hackers peuvent remporter des prix en espèces ainsi que des logiciels et du matériel qu'ils ont réussi à exploiter. C'est un concours de hacking international de recherche de vulnérabilités logicielles, lancé en 2005 par TippingPoint. Le programme a été racheté par Trend Micro dans le cadre de l'acquisition de HP TippingPoint en 2015. ZDI achète diverses vulnérabilités logicielles à des chercheurs en cybersécurité, puis divulgue ces vulnérabilités à leurs fournisseurs d'origine pour qu'ils les corrigent avant de rendre ces informations publiques.

Le terme "zero-day" fait référence à la première fois, ou jour zéro, où un fournisseur prend connaissance d'une vulnérabilité dans un logiciel spécifique. Le programme a été lancé pour récompenser en espèces les pirates informatiques qui parviennent à trouver des exploits dans n'importe quel type de logiciel. ZDI a été créée en tant que programme tiers pour collecter et encourager la découverte de telles failles, tout en protégeant à la fois les chercheurs et les informations sensibles qui se cachent derrière ces vulnérabilités.

https://www.zerodayinitiative.com/about/