SYNACKTIV

Communiqué de Presse

Les hackers de Synacktiv piratent la Tesla et remportent 200 000 $ de prime et une deuxième Tesla Model 3

L'équipe française de chercheurs en cybersécurité remporte pour la 3ème fois la compétition de piratage sur la Tesla lors du concours Pwn2Own qui se tient en ce moment à Vancouver

Paris, Vancouver, le 22 mars 2024 – L'équipe de hackers éthiques de Synacktiv remporte la compétition Pwn2Own sur le hack de la Tesla à Vancouver, après s'être illustrée sur le même modèle à Tokyo en janvier dernier.

C'est la troisième fois que Synacktiv, expert en cybersécurité offensive, réussi à compromettre la Tesla. Cette fois c'est la sécurité de l'unité de contrôle électronique (ECU) et du BUS CAN des véhicules électriques qui sont exploités. Une prouesse réalisée en moins de 30 secondes Live devant le jury du Pwn2Own à Vancouver... Cet exploit permet à l'équipe de Synacktiv de remporter une récompense de 200 000 $ et une toute nouvelle Tesla Model 3.

Tesla met en jeu ces primes afin d'encourager la recherche de potentielles failles critiques sur ses véhicules connectés. En bénéficiant des travaux de recherche d'une communauté de hackers internationaux, elle accéde aux détails des failles de sécurité qu'elle n'avait pas identifié, et que le constructeur s'engage à corriger rapidement, assurant ainsi la sécurité de ses produits et la protection des utilisateurs. Selon les règles du concours, les vulnérabilités exploitées et signalées doivent être corrigées sous 60 jours sous peine de divulgation publique.

Organisé par Zero Day Initiative (ZDI) le concours de piratage Pwn2Own vise à sensibiliser les éditeurs et constructeurs à renforcer la sécurité des véhicules connectés, et à encourager une collaboration proactive avec les chercheurs en cybersécurité à l'échelle mondiale.

A propos de Synacktiv

Fondée en 2012 par deux experts en cybersécurité, 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 200 clients et emploie actuellement une équipe de plus de 150 experts en cybersécurité. Elle opère principalement depuis ses bureaux de Paris, 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/