Jeep Cherokee piratée : Blackberry dédouane son OS embarqué QNX

A l'occasion de la conférence sur la sécurité Black Hat la semaine dernière à Las Vegas, l'ingénieur Charlie Miller et Chris Valasek, directeur de recherche sur la sécurité des véhicules chez IOActive, démontraient comment pirater une voiture connectée. Plus exactement une Jeep Cherokee de Chrysler. La démonstration a fait grand bruit lors de l'événement même si les deux hommes avaient déjà partagé le résultat de leurs travaux en amont via un essai plus que parlant publié par le magazine *Wired*.

Le logiciel qu'ils ont développé leur permet de prendre le contrôle de la Jeep à distance, par Internet, en passant par le système embarqué de gestion des fonctions multimédia du véhicule. Ventilation, affichage d'image sur l'écran du tableau de contrôle, autoradio, essuie-glaces, arrêt du véhicule, direction, fermeture/ouverture des portières… toutes les fonctions majeures de l'auto passent sous le contrôle des chercheurs, jusqu'au contrôle des freins. Et ce, sans que le conducteur puisse reprendre la main. Une prise de contrôle à distance pour le moins préoccupante pour l'ensemble des conducteurs de véhicules connectés que l'on peut voir sur cette vidéo.

Des centaines de milliers de Chrysler affectées

Si le test a été effectué sur un modèle particulier de Jeep, les chercheurs affirment que des centaines de milliers de véhicules de chez Chrysler équipés d'un tableau de bord connecté sont vulnérables. Ils en ont évidemment fait part au constructeur qui a rappelé pas moins de 1,4 million de véhicules pour installer un correctif que le propriétaire peut néanmoins appliquer lui-même. Il faut dire que Chrysler risque pas moins qu'une action de groupe en justice, qui pourrait lui coûter très cher, et que la National Highway Traffic Safety Administration (NHTSA), l'administration autoroutière américaine, s'intéresse à la question (il serait temps).

Point commun de tous ces véhicules ? Le système d'exploitation embarqué QNX Neutrino OS, développé par QNX Software Systems, une filiale de Blackberry depuis son acquisition en 2010. Mais l'éditeur défend l'intégrité de son OS. *« L'article [de Wired] se demande si la vulnérabilité n'est pas propre à la technologie QNX*, interroge faussement Blackberry dans un billet de blog posté hier, lundi 10 août. *Nous pouvons affirmer sans équivoque que ce n'est pas le cas. »*

60 millions de véhicules équipés

Pour étayer ses arguments, le constructeur canadien explique que QNX Neutrino OS a été déployé dans plus de 60 millions de véhicules et éprouvé sur le terrain dans une foule d'applications critiques. Il rejette la vulnérabilité sur des applications tierces. *« Dans ce cas particulier, la vulnérabilité provient de certains composants logiciels et de l'architecture qui ne sont pas liées à l'OS QNX Neutrino. »* Qui plus est, *« les deux chercheurs en sécurité qui ont révélé la vulnérabilité ont clairement démontré que la faille exploitée n'était pas issue de QNX Neutrino OS »*.

Charlie Miller et Chris Valasek ont en effet pointé les fonctions de connectivité implantées au-dessus de QNX plus que l'OS lui-même. Un logiciel baptisé uConnect, qui exploite le réseau cellulaire pour offrir des accès Internet, des fonctions de commandes vocales et autres services de contrôle au conducteur, est particulièrement mis en cause par les chercheurs en sécurité. Selon eux, c'est la façon dont Chrysler a implémenté uConnect qui permettrait aux pirates de prendre le contrôle du véhicule à distance, particulièrement en passant par le bus CAN, le réseau informatique interne au véhicule utilisé dans l'industrie automobile pour gérer les fonctions majeures comme le moteur ou la direction.

La voiture connectée avenir de Blackberry

En juillet dernier, Blackberry s'était déjà rapidement défendu (par tweet) de toute responsabilité dans la vulnérabilité de la Jeep. Mais un article publié le 7 août sur le site Seeking Alpha, dédié à l'actualité financière, a suggéré que l'OS embarqué du constructeur canadien pourrait être impacté par la *class action* déposée à l'encontre du groupe Fiat Chrysler et Harman International à l'origine de la solution uConnect. Bien que Blackberry ne soit pas concerné par cette action en justice, il entend tout faire pour rester à l'écart. Et pour cause : Audi, Ford, Mercedes, ou encore Volkswagen ont adopté les technologies QNX du Canadien. La plate-forme embarquée s'inscrit donc comme un élément stratégique de son développement alors que l'entreprise peine à redresser la barre sur le secteur des terminaux et services mobiles. *« La voiture connectée est l'avenir »*, affirme le constructeur. Raison de plus pour éviter une sortie de route anticipée.

Lire également

La sécurité des voitures connectées étudiée sur toutes les coutures
250 millions de voitures connectées en 2020
Hacker les voitures connectées ? C'est en Open Source