100% des montres connectées présentent des failles de sécurité | Le Net Expert Informatique

Les montres équipées de connexion réseau et de fonctions de communication représentent une nouvelle cible pour les cyberattaques. Tel est le principal résultat de l'étude, menée par HP Fortify, qui révèle que 100% des montres testées recèlent d'importantes vulnérabilités, comme par exemple des fonctions d'authentification insuffisantes, un manque de capacités de chiffrement, et des soucis dans la protection des données personnelles1. Dans ce rapport, HP recommande un certain nombre d'actions pour améliorer la sécurité dans la conception et l'utilisation des montres, à la maison ou dans son environnement de travail.

Avec le déploiement de l'Internet des Objets, les smartwatches gagnent en popularité en raison de leur côté pratique et des nouvelles fonctionnalités qu'elles proposent. En devenant des objets usuels, ces montres vont collecter de plus en plus d'informations personnelles sensibles, comme des données de santé. La possibilité de les connecter avec des applications disponibles sur smartphone risquent prochainement de leur donner accès à encore plus d'informations, comme par exemple les codes permettant d'ouvrir votre maison ou votre véhicule.
« Les montres connectées commencent à peine à entrer dans nos vies. Elles offrent déjà de nouvelles fonctionnalités innovantes qui pourraient ouvrir la voie à de nouvelles menaces sur des informations et des activités sensibles », a déclaré Jason Schmitt, Directeur Général Fortify de l'entité HP Security. « Avec l'accélération de l'adoption des smartwatches, cette plate-forme va devenir bien plus attrayante pour tous ceux qui voudraient en faire une utilisation frauduleuse. Il devient nécessaire de prendre des précautions lors de la transmission des données personnelles ou du raccordement de ces équipements aux réseaux d'entreprise. »
L'étude HP s'interroge ainsi sur la capacité des smartwatches à stocker et à sécuriser les données sensibles pour lesquelles elles ont été conçues. HP s'est appuyé sur HP Fortify on Demand pour évaluer 10 montres connectées à des applications mobiles et un cloud Android ou iOS.

Cette étude révèle de nombreuses failles de sécurité parmi lesquelles les plus fréquentes et les plus faciles à corriger sont :

L'insuffisance des fonctions d'autorisation et d'authentification des utilisateurs :
Chaque montre connectée testée était couplée à une interface sur téléphone mobile qui ne gérait pas l'authentification à deux facteurs, et qui ne verrouillait pas les comptes après 3 ou 5 saisies de mots de passe infructueux. Trois montres sur dix, c'est à dire 30%, étaient vulnérables aux tentatives de moisson de comptes utilisateurs, ce qui veut dire qu'un pirate informatique pourrait obtenir le contrôle de la montre et de ses données en profitant d'une politique de mots de passe faible, du non blocage des comptes, ou en énumérant des listes de comptes utilisateur potentiels.

Le manque de chiffrement lors du transfert de données :
Le chiffrement lors du transport d'information est essentiel, dans la mesure où des informations personnelles sont envoyées vers de multiples destinations dans le cloud. Même si 100 pourcents des montres testées intégraient le chiffrement lors transport avec le protocole SSL/TLS, environ 40% des connexions vers le cloud restaient vulnérables à l'attaque POODLE, permettant l'utilisation d'outils de déchiffrement peu puissants, ou encore le protocole SSL v2.

Interfaces peu sécurisées :
30% des montres testées utilisaient des interfaces web accessibles en mode cloud, et toutes présentaient des risques d'énumération de comptes utilisateur. Dans un test spécifique, 30% ont également révélé des risques d'énumération de comptes utilisateur depuis leurs applications sur mobile. Cette défaillance permet aux hackers d'identifier des comptes utilisateurs valides en s'appuyant sur les informations reçues via les mécanismes de réinitialisation de mots de passe.

Logiciels et microcode peu sécurisés :
70% des montres ont révélé des failles dans la protection des mises à jour de microcode, comme par exemple la transmission en clair des mises à jour, sans chiffrer les fichiers. Cependant, plusieurs mises à jour étaient protégées par une signature, évitant ainsi l'installation d'un microcode contaminé. Même si des updates malicieuses ne peuvent être installées, le manque de chiffrement permet aux fichiers d'être téléchargés puis analysés.

Soucis sur la protection des données personnelles :
Toutes les montres collectent des données personnelles – comme le nom, l'adresse, la date de naissance, le poids, le sexe, la fréquence cardiaque, et bien d'autres informations relatives à la santé de l'utilisateur. Si l'on rapproche ceci des problèmes relevés sur l'énumération des comptes utilisateur ou l'utilisation de mots de passe faiblement sécurisés sur certaines montres, le risque de diffusion des données personnelles depuis une montre connectée devient un problème réel.

En attendant que les fabricants incorporent les dispositifs nécessaires permettant de mieux sécuriser leurs smartwatches, les utilisateurs sont priés d'examiner scrupuleusement les fonctions de sécurisation existantes avant de choisir un modèle de montre connectée. HP recommande aux utilisateurs de ne pas activer les fonctions de contrôle des accès sensibles, comme par exemple l'accès à leur domicile ou leur véhicule, sauf si un mécanisme d'autorisation performant est proposé par la montre. De plus, en activant la fonctionnalité passcode, en imposant des mots de passe sophistiqués et en introduisant une authentification à deux facteurs, il est possible d'éviter des accès frauduleux aux données. Au delà de la protection des données personnelles, ces mesures sont essentielles dès lors que la smartwatch va être utilisée dans un environnement de travail et connectée au réseau de l'entreprise.

Méthodologie
Réalisée par HP Fortify, l'étude HP Smartwatch Security Study a utilisé la méthodologie HP Fortify on Demand IoT testing methodology, combinée avec des tests manuels et d'autres outils de test automatisés. Les équipements et les composants testés ont été évalués sur la base de l'outil OWASP Internet of Things Top 10 et des vulnérabilités spécifiques associées à chacune des 10 premières catégories.
Toutes les données et les tous les pourcentages inclus dans l'étude ont été extraits des tests menés sur les 10 montres évaluées. Malgré l'existence d'un nombre croissant de fabricants et de modèles de smartwatches, HP pense que les résultats obtenus sur cet échantillon de 10 modèles donne un bon indicateur du niveau de sécurité des smartwatches actuelles du marché.

Des conseils complémentaires sur la sécurisation des smartwatches sont disponibles dans le rapport complet (http://go.saas.hp.com/fod/internet-of-things)

Pour toute information complémentaire, il est possible de consulter le premier rapport de la série sur l'Internet des Objets, 2014 HP Internet of Things Research Study, qui passe en revue le niveau de sécurité des 10 objets connectés les plus courants du marché. De plus, l'étude 2015 HP Home Security Systems Report (http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-7342ENW&cc=us&lc=en) examine les 10 systèmes les plus répandus en matière de protection connectée du domicile.
(1) "HP Internet of Things Security Report: Smartwatches," HP, Juillet 2015.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.itrnews.com/articles/157450/100-montres-connectees-presentent-failles-securite.html et ITRmobiles.com