Groupe Hospitalier Bretagne Sud
Groupement de Coopération Sanitaire Clinique du Ter
E.P.S.M. J.M CHARCOT

SSiACTUS

NUMÉRO 34
06 JANVIER 2022

FRANCE - De faux pass sanitaires créés à partir de la base de données de vaccination Covid19

Une jeune lyonnaise de 23 ans a été interpellée le 7 décembre 2021, pour création frauduleuse de faux pass sanitaires, qu'elle vendait entre 50 et 100 euros. Pour ce faire, elle a déclaré avoir récupéré des informations de praticiens sur Doctolib, avant de les utiliser pour entrer sur la plateforme "vaccin-covid". Le praticien est ensuite sollicité à distance pour approuver la connexion à cette plateforme, ce qui donne ensuite accès au site Internet de la Sécurité Sociale, permettant de générer les pass sanitaires. Pour rappel s'introduire de manière illicite sur cette base de données pour créer et vendre des pass sanitaires frauduleux est passible de 5 ans d'emprisonnement et 150 000 euros d'amende. - **France 3 régions**

ÉTATS-UNIS - Fuite de données dans le système de santé public de Broward Health

Suite à une cyberattaque le 15 octobre 2021, Broward Health a révélé que l'incident avait conduit à une violation de données à grande échelle affectant 1 357 879 personnes. Le FBI et le département de la justice des États-Unis ont été notifiés de l'incident le 19 octobre, jour de sa découverte. L'enquête a révélé que des informations telles que les nom, date de naissance, adresse physique, informations bancaires ou financières et numéro de sécurité sociale ont été divulguées. Broward Health confirme l'exfiltration des données mais précise qu'il n'y a aucune preuve d'utilisation à mauvais escient par les acteurs de la menace. Une hypothèse est émise sur le point d'intrusion : il s'agirait d'un fournisseur médical tiers autorisé à accéder au système pour fournir ses services. - **Bleeping Computer**, **Office of the Maine Attorney General**

MONDE - Découverte d'une vulnérabilité dans Uber permettant d'envoyer des courriels malveillants

Une vulnérabilité dans le système de messagerie d'Uber permettrait à n'importe qui d'envoyer des courriels au nom d'Uber. Le chercheur qui a découvert cette faille prévient qu'elle peut être exploitée par des attaquants pour envoyer des courriels à 57 millions d'utilisateurs et de chauffeurs d'Uber dont les informations ont été divulguées lors de la violation de données de 2016. Ces courriels, envoyés depuis les serveurs d'Uber, semblent légitimes aux yeux d'un fournisseur de services de messagerie (car ils le sont techniquement) et passent au travers des filtres anti-pourriel. Uber semble être au courant de la faille mais ne l'aurait pas corrigée pour le moment. - **Twitter**

MONDE - Vulnérabilité persistante de déni de service dans le produit HomeKit d'Apple

Trevor Spiniolas indique avoir découvert un bogue de déni de service dans les produits HomeKit d'Apple présent dans les versions 14.7 à 15.2 d'iOS. Le bogue a été baptisé doorLock. Le chercheur indique avoir averti Apple il y a quatre mois mais la vulnérabilité n'a pas été corrigée malgré la récente mise à jour. Un attaquant pourrait déclencher le bogue en remplaçant le nom d'un appareil HomeKit par une chaîne de plus de 500 000 caractères. Lors du chargement de la chaîne, les appareils iOS redémarreront et seront inutilisables. Des démonstrations de faisabilité (PoC) sont disponibles sur YouTube. Actuellement, désactiver les appareils domestiques dans le centre de contrôle est la seule mitigation possible. - **Trevor Spiniolas**, **Security Affairs**

FRANCE - Sanction de Free Mobile à hauteur de 300 000 euros par la CNIL

Le mardi 4 janvier 2022, la CNIL a sanctionné Free Mobile pour non-respect du RGPD. Quatre manquements ont été retenus suites à plusieurs plaintes concernant les demandes de droits d'accès aux données personnelles des utilisateurs et les demandes au droit d'opposition à recevoir des messages de prospection commerciale. La société a également continué à envoyer des factures concernant des lignes téléphoniques dont l'abonnement était résilié. Enfin, Free Mobile a transmis par mail à ses nouveaux adhérents des mots de passe non temporaires en clair lors de leur souscription à une offre, sans qu'il ne soit exigé de changement. On peut noter que l'amende est à caractère publique, puisque la CNIL souhaite souligner l'importance de traiter les demandes de droits des personnes, ainsi que la sécurité de leurs données. - **Légifrance**, **ZDNet**, **CNIL**

VALENTIN THIRION
DANA HUSSEIN HASSAN