UTILISATION DE LA TECHNOLOGIE BLUETOOTH

MAI 2021

ITSAP.00.011

Plusieurs dispositifs professionnels et personnels font appel à la technologie Bluetooth. Le Bluetooth est une technologie sans fil qui permet de transférer et de synchroniser les données entre les dispositifs sans avoir recours à des câbles physiques (p. ex. d'un portable à un casque d'écoute, à un moniteur d'activité et à une application). Il est également utilisé pour assurer le bon fonctionnement des applications de notification à l'exposition avec distribution de signal, comme Alerte COVID. À mesure qu'évolue la technologie Bluetooth, de nouvelles versions permettent d'accroître la vitesse et la portée des transferts de données entre les dispositifs. En d'autres mots, il s'agit d'une façon efficace et peu coûteuse de connecter vos dispositifs. Les auteurs de menace peuvent toutefois exploiter les vulnérabilités liées à cette technologie pour accéder à vos dispositifs et voler de l'information sensible.

CONSIDÉRATIONS EN MATIÈRE DE SÉCURITÉ LIÉES À L'UTILISATION DE BLUETOOTH

UTILISATION DES VERSIONS MISES À JOUR DE BLUETOOTH

Les dispositifs qui font appel à des versions antérieures de Bluetooth n'offrent pas les mêmes fonctions de sécurité, ce qui les rend vulnérables aux interceptions et aux attaques. Si vous connectez deux dispositifs et que l'un d'entre eux utilise une version plus ancienne de Bluetooth, la connexion en entier sera vulnérable. Bien que les mesures de sécurité des versions plus récentes de Bluetooth aient été améliorées, vous devriez faire preuve de prudence lorsque vous utilisez cette technologie.

PROTECTION DE L'INFORMATION SENSIBLE

Évitez de transférer l'information sensible par l'intermédiaire de connexions Bluetooth. Il convient, par exemple, de ne pas utiliser de claviers compatibles Bluetooth pour saisir de l'information sensible ou des mots de passe, puisque cette information peut être interceptée (p. ex. enregistrement de la frappe). Lorsque vous utilisez la technologie Bluetooth, comme une souris sans fil, gardez à l'esprit que votre ordinateur sera vulnérable aux attaques à distance advenant l'exploitation ou la compromission de l'adaptateur sans fil de la souris, qui sert à établir la connexion Bluetooth.

DÉSACTIVATION DU MODE DÉCOUVERTE

Le mode Découverte est un état dans lequel un dispositif compatible Bluetooth peut chercher d'autres dispositifs à proximité et s'y connecter. Si vous utilisez le mode Découverte pour connecter vos dispositifs, vous devriez seulement vous connecter à des dispositifs de confiance que vous connaissez. Désactivez le mode Découverte lorsque vous ne l'utilisez pas.

UTILISATION DE DISPOSITIFS APPLIQUANT LES MESURES DE SÉCURITÉ APPROPRIÉES

Choisissez des dispositifs Bluetooth utilisant des mécanismes de sécurité, comme des mots de passe modifiables. Certains produits Bluetooth n'utilisent pas de NIP ou de mots de passe, ou utilisent des mots de passe fixes (p. ex. le NIP0000). Les mots de passe modifiables font en sorte qu'il est plus difficile pour un auteur de menace de se connecter à vos dispositifs et d'y accéder.

AUTHENTIFICATION ET AUTORISATION DES DISPOSITIFS

Protégez vos dispositifs et votre information en authentifiant et autorisant les autres dispositifs. Vérifiez toujours que le dispositif affiché correspond bien à un dispositif de confiance que vous connaissez avant de le jumeler au vôtre. Pour autoriser et vérifier les connexions, on utilise des codes de jumelage et des clés d'accès. Méfiez-vous si vous recevez une demande de jumelage dont vous n'êtes pas à l'origine. Rappelez-vous qu'une fois jumelés, les dispositifs restent sur votre liste de dispositifs jumelés. Supprimez toujours les dispositifs perdus ou volés de votre liste de dispositifs jumelés.

VOITURES COMPATIBLES BLUETOOTH

Connecter des dispositifs à des voitures compatibles Bluetooth permet aux conducteurs et aux passagers de faire des appels mains libres, d'envoyer des textos ou des courriels, d'écouter de la musique et de se connecter à Internet. Vos renseignements personnels sont stockés dans le système de la voiture au moment où vous jumelez votre dispositif. Il est possible d'accéder à vos journaux d'appels, à vos contacts et à vos messages, comme les textos, les courriels ou toute messagerie basée sur une application, à partir de l'écran de votre voiture au moyen de Bluetooth. Si vous êtes propriétaire de la voiture en question, vous pourriez penser que ce n'est pas vraiment un problème, mais qu'adviendra-t-il lorsque vous vendrez votre voiture ou si vous louez un véhicule? Assurez-vous de supprimer vos données et vos dispositifs au moment où vous vendez votre voiture. Il est préférable d'éviter de jumeler vos dispositifs avec des voitures en location. Si vous devez effectuer un appel mains libres dans une voiture de location, utilisez le haut-parleur intégré de votre dispositif ou jumelez votre dispositif à un dispositif Bluetooth personnel.

SÉRIE SENSIBILISATION

MENACES DONT IL FAUT TENIR COMPTE

Les dispositifs compatibles Bluetooth sont vulnérables aux cybermenaces générales. Les auteurs de menace utilisent différentes techniques d'attaque pour se connecter à vos dispositifs, écouter secrètement vos conversations et voler votre information. Voici quelques-unes de ces techniques :

Attaque du protocole : Un auteur de menace transmet des paquets (p. ex. de petites parties de données) ou se fait passer pour un dispositif en vue de contourner les mécanismes d'authentification et de chiffrement.

Attaque par déni de service (DoS) : Un auteur de menace bloque le signal pour empêcher votre dispositif de se connecter à un autre dispositif. Les attaques par DoS sont souvent combinées aux attaques du protocole pour refuser l'accès aux dispositifs voulus et les rediriger vers un dispositif trafiqué.

Une fois que l'auteur de menace s'est connecté à votre dispositif, il peut mener de plus amples attaques. En voici des exemples :

Attaque par écoute clandestine : Un auteur de menace capture et décode de l'information sensible dans vos transmissions Bluetooth (p. ex. mot de passe saisi sur un clavier Bluetooth).

Attaque par usurpation d'identité : Un auteur de menace mène une attaque par mystification ou une attaque de l'intercepteur pour accéder au contenu et aux services de votre dispositif dans le but d'en télécharger le contenu et de modifier les paramètres. Les dispositifs de l'Internet des objets sont souvent vulnérables à ces types d'attaques.

En plus d'utiliser ces techniques, les auteurs de menace peuvent tirer avantage des vulnérabilités liées aux dispositifs, aux logiciels et aux applications pour accéder à vos dispositifs Bluetooth et en obtenir le contrôle. Advenant la compromission de votre dispositif, les auteurs de menace peuvent voler l'information, faire le suivi de vos déplacements et modifier les paramètres du dispositif à votre insu.

Pour atténuer les vulnérabilités et vous protéger des cybermenaces, il convient d'appliquer les plus récentes mises à jour à vos dispositifs, vos logiciels et vos applications. Assurez-vous d'appliquer régulièrement les mises à jour et les correctifs.

Pour de plus amples conseils sur la façon d'assurer la sécurité de vos dispositifs, consultez le document *ITSAP.00.001, Utiliser son dispositif mobile en toute sécurité*.

RÉSUMÉ DES CONSEILS EN MATIÈRE DE SÉCURITÉ

La technologie Bluetooth est en constante évolution, mais quelques étapes simples vous permettront de protéger vos données et vos dispositifs :

- Appliquez les plus récentes mises à jour à tous les dispositifs Bluetooth (p. ex. téléphones, casques d'écoute, claviers, consoles de jeu);
- Désactivez le Bluetooth lorsque vous ne l'utilisez pas*;
- Désactivez le mode Découverte lorsque vous n'avez pas à connecter de dispositifs;
- Évitez de jumeler des dispositifs dans des espaces publics;
- Ne jumelez votre dispositif qu'à des dispositifs de confiance que vous connaissez;
- Ne transférez jamais l'information sensible par l'intermédiaire de connexions Bluetooth;
- Évitez d'utiliser des claviers compatibles Bluetooth pour saisir de l'information sensible ou des mots de passe;
- Supprimez les dispositifs perdus ou volés de votre liste de dispositifs jumelés;
- Supprimez toutes les données et dispositifs enregistrés dans les voitures compatibles Bluetooth;
- Évitez de jumeler des dispositifs avec des voitures de location.

***Remarque :** Les applications de notification à l'exposition (p. ex Alerte COVID) exigent l'activation continue du Bluetooth. Dans un tel cas, vous devriez envisager de supprimer tous les dispositifs jumelés que vous n'utilisez pas et de limiter les autorisations sur votre dispositif.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.