CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Utilisation de la technologie Bluetooth

Avril 2024

ITSAP.00.011

Le Bluetooth est une technologie sans fil qui a recours à la radiofréquence pour transférer et synchroniser des données entre des dispositifs sur une courte distance, comme un ordinateur portable et un casque d'écoute sans fil. 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. S'il est vrai qu'il s'agit d'une façon économique et efficace de connecter vos dispositifs, il faut savoir que les auteures et auteurs de menace peuvent exploiter les vulnérabilités de la technologie Bluetooth pour avoir accès à vos dispositifs et voler de l'information sensible.

Considérations en matière de sécurité liées à l'utilisation de Bluetooth

Voici quelques exemples de mesures de sécurité à prendre en considération avant d'utiliser la technologie 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

Lorsque vous utilisez la technologie Bluetooth, gardez à l'esprit que votre ordinateur sera vulnérable aux attaques à distance. 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, car cette information peut être interceptée.

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.

Authentification et autorisation des dispositifs

Protect 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. Vous pouvez utiliser des codes de jumelage et des clés d'accès pour autoriser et vérifier les connexions sans fil. 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 et qu'ils vont souvent se connecter automatiquement lorsqu'ils sont à portée et activés.

Déconnexion d'anciens dispositifs

Gardez votre liste de jumelages Bluetooth à jour. Cette liste se trouve dans les paramètres Bluetooth de votre dispositif. Évitez les jumelages temporaires, comme la connexion à un haut-parleur dans un logement loué à court terme; vous pourrez ainsi prévenir des risques inutiles liés à la sécurité. Supprimez les dispositifs perdus ou volés de votre liste de jumelages le plus rapidement possible.

Méfiez-vous de votre environnement

Lors du premier jumelage entre deux dispositifs, effectuez celui-ci à partir d'un lieu sécurisé afin de réduire les risques de piratage de votre dispositif. Faites attention aux personnes avec qui vous vous connectez et refusez toutes les demandes de connexions inconnues. **Vous devriez désactiver la fonction Bluetooth lorsqu'elle n'est pas utilisée.**

SÉRIE SENSIBILISATION

No de cat. D97-1/00-011-2024F-PDF
ISBN 978-0-660-7089-1

Canada

Menaces liées à la technologie Bluetooth

Les dispositifs compatibles Bluetooth sont vulnérables aux cybermenaces générales. Les auteures et auteurs de menace utilisent différentes techniques d'attaque pour se connecter à vos dispositifs, écouter secrètement vos conversations et voler votre information. Voici des exemples de méthodes d'attaque couramment constatées :

Attaque du protocole : Une auteure ou un auteur de menace transmet des paquets, comme de petites parties de données, ou se fait passer pour un dispositif en vue de contourner les mécanismes d'authentification et de chiffrement.

Intrusion Bluetooth : Une auteure ou un auteur de menace envoie un message non sollicité à vos dispositifs mobiles compatibles Bluetooth. Si vous répondez au message ou ajoutez le contact à votre carnet d'adresses, vous donnez à l'auteure ou auteur de menace l'occasion de se connecter à vos dispositifs, car vous l'établissez en tant que contact connu. Les auteures et auteurs de menace peuvent alors contrôler votre dispositif à distance.

Attaque par déni de service (DoS) : Une auteure ou 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'auteure ou auteur de menace s'est connecté à votre dispositif, il peut mener de plus amples attaques, comme :

- **Attaques par écoute clandestine :** Une auteure ou un auteur de menace capture et décode de l'information sensible dans vos transmissions Bluetooth, comme un mot de passe saisi sur un clavier Bluetooth.

- **Attaque par usurpation d'identité :** Une auteure ou 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 auteures et 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 en savoir plus

- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)
- Conseils de sécurité pour les dispositifs périphériques (ITSAP.70.015)
- Dispositifs mobiles et voyages d'affaires (ITSAP.00.087)

Voitures compatibles Bluetooth

Connecter des dispositifs à des voitures compatibles Bluetooth permet aux occupants et occupants de faire des appels mains libres, d'envoyer des textos, d'écouter de la musique Vos renseignements personnels (journaux d'appels, contacts, messages, etc.) sont stockés dans le système de la voiture au moment où vous jumelez votre dispositif. Si vous êtes propriétaire de la voiture en question, vous pourriez penser que ce n'est pas vraiment un problème, mais cela peut devenir préoccupant si vous vendez 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 téléphone à un dispositif Bluetooth personnel.