La minute du PSIR

05 2025 - # 72

Bluesnarfing

NIVEAU DE DIFFICULTÉ

Cybersécurité

PERSONNES CONCERNÉES

Le Bluetooth est une technologie de communication sans fil largement répandue, utilisée pour connecter divers appareils électroniques sur de courtes distances, comme les casques audios, smartphones, claviers, souris ou même les systèmes embarqués des véhicules. Son utilité réside dans la simplification des connexions entre appareils proches, offrant ainsi une grande commodité d'utilisation.

Le Bluetooth présente des aspects liés à la sécurité qui méritent attention. Parmi les risques identifiés, l'une des menaces est connue sous le nom de **Bluesnarfing**.

Le terme **Bluesnarfing** désigne une forme d'attaque qui vise à **accéder et à copier des données présentes sur un appareil compatible Bluetooth, sans l'autorisation de son propriétaire et souvent à son insu**. L'objectif principal de cette attaque est le **vol d'informations**.

Concrètement, un acteur malveillant exploitant une vulnérabilité de sécurité dans l'implémentation du protocole Bluetooth sur un appareil cible peut parvenir à établir une connexion non autorisée. Une fois cette connexion établie, il peut alors extraire diverses données sensibles stockées sur l'appareil. Les informations typiquement ciblées par le Bluesnarfing incluent, sans s'y limiter :

- Le **répertoire téléphonique** ou la liste de contacts.
- Les **messages** (SMS, parfois des éléments de courriels ou de journaux d'appels).
- Des **fichiers multimédias** tels que des photos ou des vidéos.

Il est important de noter que pour réaliser une attaque de Bluesnarfing, l'attaquant doit généralement se trouver à proximité physique de l'appareil ciblé, à portée du signal Bluetooth (qui est d'une dizaine de mètres).

Mesures de sécurité :

Pour se prémunir contre le risque de Bluesnarfing, il est conseillé d'appliquer des mesures de sécurité simples :

1. **Désactiver la fonction Bluetooth** sur vos appareils lorsque vous n'en avez pas besoin.
2. **Rendre votre appareil "non détectable"** (ou "non visible") dans les paramètres Bluetooth, afin qu'il n'apparaisse pas lors d'un scan par des appareils inconnus, sauf pendant la procédure de jumelage active d'un nouvel équipement.
3. **Maintenir à jour le système d'exploitation** de vos appareils (smartphones, ordinateurs portables, etc.) ainsi que les microprogrammes des périphériques Bluetooth. Les mises à jour de sécurité corrigent les vulnérabilités connues.

En adoptant ces précautions, vous réduisez significativement l'exposition de vos appareils à ce type d'attaque et protégez vos données personnelles.

Pour plus d'information