ALERTE n°BA17-02

WPA/WPA2 : Une faille majeure dans le protocole de sécurisation du Wi-Fi.

Date de publication : 17/10/2017

Systèmes affectés

La vulnérabilité touche entre autres les systèmes suivants :

- Windows ;
- Linux ;
- Android ;
- Apple.

Aperçu

Le CIRT-BF a pris connaissance de l'existence de plusieurs vulnérabilités majeures dans protocole de sécurité Wi-Fi Protected Access II (WPA2). Elles permettent à des pirates d'intercepter le trafic Wi-Fi entre les ordinateurs et les points d'accès.

Description

Wi-Fi Protected Access (WPA/WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type Wi-Fi. Il est censé garantir la sécurité de tout ce qui transite entre un terminal (ordinateur ou smartphone) et un point d'accès.

Cependant lors de l'établissement d'une session de communication utilisant ce protocole, il est possible d'interférer sur le mécanisme en quatre temps visant à assurer la confidentialité des échanges. Lors de cette phase d'initialisation, un utilisateur malveillant interceptant les communications entre un client et un point d'accès Wi-Fi, peut amener le client à réutiliser des paramètres entrant en compte dans le chiffrement des données échangées. Cela peut permettre à un attaquant de provoquer une atteinte à la confidentialité ou à l'intégrité des données. Par ailleurs, l'implémentation du protocole dans les logiciels wpa_supplicant rend l'exploitation de la vulnérabilité particulièrement aisée. Dans ces conditions il est notamment possible de rejouer des paquets réseau, d'injecter du contenu vers un client connecté en Wi-Fi et d'accéder à des communications confidentielles. Si tous les clients utilisant WPA/WPA2 sont vulnérables à cette attaque, les objets connectés, les appareils sous Linux et Android sont

particulièrement sensibles de par l'utilisation native de wpa_supplicant. On notera qu'afin de pouvoir réaliser ces attaques sur WPA/WPA2 un attaquant doit nécessairement être à proximité du réseau Wi-Fi cible. De plus, il est à noter que ces attaques ne compromettent pas la clé Wi-Fi et qu'une modification de cette clé ne permet pas de se prémunir de l'attaque.

Impact

Hautement critique, l'exploitation de cette faille permet le décryptage, la relecture de paquets, le piratage de connexion TCP, l'injection de contenu HTTP et autres. Notez qu'en tant que failles détectées au niveau du protocole, la plupart voire toutes les implémentations correctes du standard seront affectées.

Solution

Bien que cela paraisse compliqué, voire impossible, la seule recommandation qu'il est possible d'effectuer à ce jour, c'est d'éviter d'utiliser le Wi-Fi autant que possible jusqu'à ce qu'un patch soit en place. Par ailleurs, CIRT-BF recommande aux utilisateurs de :

- mettre à jour régulièrement tout système se connectant au réseau Wi-Fi (Systèmes industriels, objets connectés, postes clients, répéteurs Wi-Fi, etc.), en s'appuyant sur la liste des systèmes affectés ci-dessous ;
  https://www.kb.cert.org
- privilégier les protections de type TLS ou VPN pour assurer l'intégrité et la confidentialité des données échangées sur les réseaux Wi-Fi ;
- configurer les équipements Wi-Fi pour imposer l'utilisation de WPA2 (et non pas WPA) et AES-CCMP (et non pas TKIP) ; cette recommandation ne permet pas de se prémunir contre une potentielle écoute d'une communication mais empêche le vol de la clé de session Wi-Fi ;
- désactiver ou filtrer le trafic multicast ; ce type de trafic rendant les systèmes Microsoft et Apple vulnérables.

Références

- Page internet décrivant l'attaque sur le protocole WPA/WPA2
  https://www.krackattacks.com/
- Liste des systèmes affectés par la vulnérabilité WPA2
  https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4
- Référence CVE CVE-2017-13077
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13077
- Référence CVE CVE-2017-13078
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13078
- Référence CVE CVE-2017-13079
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13079
- Référence CVE CVE-2017-13080
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13080
- Référence CVE CVE-2017-13081
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13081
- Référence CVE CVE-2017-13082
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13082

- Référence CVE CVE-2017-13084
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13084
- Référence CVE CVE-2017-13086
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13086
- Référence CVE CVE-2017-13087
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13087
- Référence CVE CVE-2017-13088
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13088

Révisions

- 16 oct. 2017– *Date de première publication*

[Télécharger (193 Ko)]