Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 18 OCT. 2017
N° 5111 /ANSSI/COSSI

Note
à
destinataires *in fine*

Objet : Découverte d'une vulnérabilité importante concernant le protocole WPA/WPA2.

Référence : Avis du CERT-FR ALE014 du 16 octobre 2017.

1 Contexte

Le 16 octobre 2017, des chercheurs en sécurité ont publié un avis de vulnérabilité nommé **KRACK** (*Key Reinstallation Attacks*), la méthode dévoilée permet le décryptement[1] suite à l'interception d'une communication sans fil utilisant les protocoles WPA/WPA2. Dans certains cas une altération des données est possible.

2 Nature et impact de la vulnérabilité

La faille découverte se situe dans la phase de connexion d'un client à un réseau Wi-Fi sécurisé par les protocoles WPA/WPA2. Une faiblesse de la spécification de la phase d'initialisation de la connexion diminue la sécurité cryptographique de la session, pouvant entraîner une atteinte à la confidentialité, voire à l'intégrité des données transmises. Cette attaque ne permet en revanche pas d'accéder aux réseaux informatiques connectés à la borne Wi-Fi.

Par ailleurs, l'implémentation du protocole dans les logiciels *WPA Supplicant* rend l'exploitation de la vulnérabilité particulièrement aisée, permettant notamment de prendre le contrôle de connexions réseau, de rejouer des paquets IP, d'injecter du contenu réseau vers un client connecté en Wi-Fi, et ainsi d'accéder à des communications confidentielles.

Tous les clients utilisant WPA/WPA2 sont vulnérables à cette attaque ; les objets connectés, les appareils sous LINUX et ANDROID sont particulièrement touchés de par l'usage natif de *WPA Supplicant*.

Il est à craindre qu'aucun correctif sécurité ne soit jamais disponible pour les systèmes industriels, ANDROID OEM. Le cas échéant, la désactivation du Wi-Fi reste la seule façon de se prémunir de ce type d'attaque.

Cependant, un attaquant doit nécessairement être à proximité du réseau Wi-Fi et disposer d'équipements informatiques spécifiques pour exploiter cette vulnérabilité.

Le changement de clef ne permet pas de se prémunir de l'attaque.

[1] Récupération du clair sans posséder la clé.

3 Recommandations prioritaires

Le CERT-FR recommande plusieurs mesures afin de limiter l'impact de cette vulnérabilité :

- mettre à jour régulièrement tout système se connectant au réseau Wi-Fi (systèmes industriels, objets connectés, ordiphones, postes clients, répéteurs Wi-Fi), en s'appuyant sur les liens présentés au chapitre 5 ;
- 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 de se prémunir contre une potentielle écoute d'une communication, mais empêche le vol de la clef de session Wi-Fi ;
- désactiver ou filtrer le trafic *multicast* ; ce type de trafic rendant les systèmes *MICROSOFT* et *APPLE* vulnérables ;
- faire un inventaire et une analyse de risque des systèmes utilisant un réseau Wi-Fi, notamment des systèmes cités plus haut, afin de désactiver si possible le service Wi-Fi.

4 Recommandations générales

Le CERT-FR, dans le cadre de cette alerte, rappelle les bonnes pratiques suivantes :

- assurer une veille des publications de correctifs de sécurité des composants cités *supra* ;
- sensibiliser les utilisateurs, notamment ceux particulièrement ciblés et manipulant des informations sensibles, aux risques liés à l'utilisation de réseau Wi-Fi (public ou non) ;

5 Liens

Le bulletin d'alerte du Cert-Fr sera régulièrement mis à jour (alerte ALE-14 du Cert-Fr https://www.cert.ssi.gouv.fr/alerte/CERTFR-2017-ALE-014).

Une description technique de l'attaque est présentée sur le site suivant :

- Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, https://www.krackattacks.com/
- Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 (Paper), http://papers.mathyvanhoef.com/ccs2017.pdf

La liste des produits concernés est tenue à jour par le *CERT Coordination Center* sur le lien suivant :

- WPA2 handshake traffic can be manipulated to induce nonce and session key reuse, www.kb.cert.org/vuls/id/228519

Bruno MARESCAUX
Sous-directeur, chef du
Centre opérationnel de la SSI