Une faille d'un client WiFi expose Android, Linux et BSD

L'Open Source Software Security (OSS-Security) a alerté sur l'existence d'une faille dans wpa_supplicant, le composant multiplateforme utilisé pour contrôler les connexions WiFi en mode WPA et WPA 2. Les plateformes concernées sont Android, Linux et BSD qui intègrent nativement ce composant. On peut le trouver également sur des solutions tierces pour les systèmes d'exploitation Mac OS X et Windows.

La vulnérabilité a été découverte par une équipe de chercheurs du groupe Alibaba. Elle a transmis le fruit de ses travaux aux développeurs en charge de la sécurité de wpa_supplicant. Dans le détail, la faille provient de la façon dont wpa_supplicant analyse les informations du SSID (Service Set Indentifier) issues des trames du réseau WiFi quand l'option Config_P2P est activée. En exploitant cette vulnérabilité, des attaquants peuvent saturer le client par déni de service, lire le contenu des processus mémoire ou injecter du code malveillant dans la mémoire.

Toutes les versions de wpa_supplicant de 1.0 à 2.4 sont vulnérables. Un correctif a été poussé en milieu de semaine et les éditeurs des systèmes d'exploitation devraient rapidement mettre à jour leur produit. En attendant les correctifs, la meilleure solution est de désactiver P2P pour chaque interface de réseau sans fil dans le client wpa_supplicant. Nos confrères de *Computerworld* notent toutefois que ce client est aussi utilisés dans les systèmes embarqués pour lesquels les correctifs ne sont pas souvent publiés ou faciles à installer.

A lire aussi :

Le WiFO, du Wifi enrichi à la lumière
Wifiphisher : un outil pour pirater tous les réseaux Wifi