Attention, faille découverte dans les réseaux mobiles GSM et 4G LTE !

Attention, faille découverte dans les réseaux mobiles GSM et 4G LTE !

Un audit de sécurité a trouvé une faille critique dans un compilateur de code utilisé par plusieurs logiciels propres aux réseaux mobiles GSM et 4G LTE

Plusieurs logiciels pour la gestion et l'interconnexion des réseaux mobiles du monde entier GSM et LTE (4G) sont vulnérables à une faille permettant une exécution de code à distance où un attaquant peut donc prendre le contrôle d'un équipement réseau. Le CERT-US a déjà lancé un avertissement sur cette vulnérabilité.

Classée sous le nom CVE-2016-5080, cette faille a été découverte lors d'un audit de sécurité d'Objective Systems, un éditeur américain qui commercialise asn1C, un compilateur de code servant à créer les applications de gestion et d'interconnexion des réseaux mobiles. Asn.1 (Abstract Syntax Notation One) est une norme internationale qui décrit les structures de données et les protocoles de transfert utilisés dans le domaine des télécommunications. Asn1c est une application qui récupère les instructions, les opérations et les structures des données pour le convertir en C, C++, C# ou en Java. Cette transformation peut ensuite être intégrée dans des applications fonctionnant sur des réseaux mobiles GSM ou LTE.

Peu d'acteurs concernés par la faille ?

Objective Systems précise que la vulnérabilité se trouve dans la compilation du code ASN.1 vers C et C++. La faille consiste en un débordement de la mémoire tampon ouvrant la porte aux attaquants pour exécuter du code sur les systèmes compromis, à distance et sans avoir besoin d'authentification sur le périphérique. L'éditeur a corrigé son logiciel et continue à vérifier la compilation vers C# et Java.

La question est de savoir qui est touché par cette faille. Le Cert américain a lancé son avertissement auprès de 34 opérateurs mobiles et équipementiers. Peu ont répondu à cet appel, Qualcomm a indiqué dans qu'il intégrait ce code dans ses produits cellulaires, mais que la faille n'est pas exploitable. Malgré cet optimisme, la société américaine a diffusé le patch d'Objective Systems sur ses solutions. D'autres entreprises comme HPE ou Honeywell ont précisé qu'elles n'étaient pas concernées.

Objective Systems revendique une base client comprenant plusieurs grands noms des réseaux mobiles comme Alcatel-Lucent, AT&T, BT, Cisco, Deutsche Telekom, etc. Le problème est qu'à la différence d'un terminal mobile, il est plus difficile de patcher les équipements télécoms.

Article original de Jacques Cheminat

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Une faille découverte dans les réseaux mobiles GSM et 4G LTE