Une application mobile fait sauter la banque

	Une application mobile fait sauter la banque

Un chercheur en sécurité a découvert une faille critique dans une application mobile d'une banque indienne. Il aurait pu pirater l'ensemble des fonds de la banque.

Sathya Prakash aurait pu devenir l'Arsène Lupin indien en braquant 25 milliards de dollars juste en piratant l'application mobile d'une banque indienne. Mais à défaut d'être un gentlemen cambrioleur, il est chercheur en sécurité et a découvert plusieurs failles dans cette application. Dans un blog, il explique disposer d'un compte dans un établissement bancaire du secteur public. Ce dernier a décidé depuis une dizaine d'années de prendre un virage vers les nouvelles technologies.

En 2015, cette banque a décidé de publier une application mobile pour iOS et Android. Par une journée pluvieuse, le chercheur connu sous le pseudo Boris s'est donc penchée sur la sécurité de cette application. Il l'a passée au peigne fin avec des solutions de débogage pour en connaître les dessous. Lors de ce premier tour d'analyse, il a constaté des faiblesses dans certains paramètres de sécurité standards, comme la gestion du HPKP (HTTP Public Key Pinning), un mécanisme de sécurité qui protège les sites internet de l'usurpation d'identité contre les certificats frauduleux émis par des autorités de certification compromises.

Code bâclée et MiTM à la clé

Or cette fonction n'était pas utilisée par l'application. Un risque pouvant conduire à une attaque de type MiTM (Man in the Middle ou Homme du milieu) et intercepter le trafic vers et depuis la banque même s'il était chiffré et transmis en HTTPS. Il a réussi à rétrograder le chiffrement SSL de version 3 à la version 2 plus vulnérable.

Ce n'est pas tout, l'application comporte aussi des négligences dans son architecture ou tout du moins une « *révision de code bâclée* ». C'est notamment le cas pour les sessions utilisateurs qui ne comprennent pas de limite dans la durée. Traditionnellement, quand un utilisateur est inactif, il est automatiquement déconnecté et il doit initier une nouvelle session. Pas dans ce cas où le chercheur parle de sessions*« immortelles »*. En combinant ce défaut avec une attaque de type MiTM, une personne peut être en mesure de réaliser des opérations pour le compte d'un utilisateur sans avoir besoin de s'authentifier à chaque fois.

Un siphonage en règle

Enfin cerise sur le gâteau. Sathya Prakash a découvert comment l'application administre les transactions bancaires. En se penchant sur les paramètres des requêtes web, il a fait de l'ingénierie inversée et trouvé un moyen pour envoyer de l'argent d'un compte à un autre. Tout cela sans authentification. Cela signifie qu'il aurait pu siphonner la totalité des dépôts de la banque, s'élevant en 2015 à 25 milliards de dollars.

Ayant des principes et de la morale, Sathya Prakash a envoyé un mail à la banque pour lui indiquer les faiblesses et les moyens de résoudre les problèmes. La banque a pris du temps pour répondre, mais est finalement intervenue au bout de 12 jours. Dans son blog, on sent le chercheur un peu aigri de ne pas avoir reçu de primes pour ses découvertes. « *Bug Bounty = 0 dollars, Welcome to India !* », conclut-il.

Article original de Jacques Cheminat

Réagissez à cet article

application mobile fait sauter la banque