La sécurité de Google perce les solutions de FireEye

Ce n'est pas la première fois qu'un éditeur de solutions de sécurité IT est concerné par des failles dans ses produits. En septembre dernier, FireEye avait été mis à l'index par un hacker qui revendiquait la découverte de 4 failles zero day et évoquait les travaux d'un autre spécialiste qui en aurait trouvé une trentaine. Aujourd'hui, c'est l'équipe de Project Zero de Google qui a percé les appliances de FireEye.

Dans un billet de blog, Travis Ormandy explique que les produits de la gamme NX, FX, AX et EX de FireEye sont concernés par cette vulnérabilité. Il rappelle que ces appliances sont parties intégrantes du réseau de l'entreprise pour surveiller le trafic comme les mails, les pièces jointes, etc. Des documents sensibles convoités par les cybercriminels. La faille découverte par Travis Ormandy et Natalie Silvanovitch a été baptisée « 666 », en référence au nombre d'avis de sécurité publié par l'équipe.

Une faiblesse dans la décompilation des JAR

La brèche se trouve dans MIP (Malware Input Processor), un module qui analyse et qui décompile les fichiers JAR, un fichier au format ZIP qui est utilisé pour distribuer un ensemble de classes Java. Les experts ont constaté une faiblesse dans la décompilation via un fichier JAR comprenant des commandes shell arbitraires et capables d'être diffusées par l'interface de surveillance passive des appliances FireEye.

Les spécialistes sont formels, un simple mail trompeur envoyé à un collaborateur pour l'amener à cliquer sur un lien malveillant suffit à ouvrir la faille et procéder à une élévation de privilège. La gamme de méfaits est ensuite vaste allant du vol de données, à l'inoculation d'un ver ou le sabotage d'un système. FireEye a été coopératif assure l'équipe de sécurité de Google. La firme américaine a travaillé pour mettre en place d'abord un outil d'atténuation du risque sur les systèmes concernés via une mise à jour automatique. Elle a délivré un correctif complet en début de semaine et conseille à ses clients de l'installer sans plus attendre.

A lire aussi :

FireEye tente de museler les chercheurs de failles

FireEye, Microsoft et consorts identifient un vaste réseau de cyberespionnage chinois

crédit photo © drx – Fotolia.com