Attention à l'arnaque de la nouvelle faille Heartbleed

L'autre faille Heartbeed, soi-disant **découverte par un groupe de pirates** la semaine dernière, se révèlerait être une arnaque pure et simple. Baptisé BitWasp, le groupe en question se propose, sur Pastebin, de vendre le kit d'exploitation de la nouvelle vulnérabilité qu'il aurait découvert après 14 jours de recherche et codage à marche forcée. **Mais l'*exploit* en question serait bidon** et la faille affectant la nouvelle version d'Open SSL inexistante.

Une faille corrigée

Rappelons que le protocole de chiffrement de la bibliothèque open source Open SSL avait été victime d'une vulnérabilité de gestion de la mémoire qui permet de récupérer jusqu'à 64 Ko de données en clair (dont les mots de passe, les numéros de carte bancaire, les certificats numériques, etc.). **Faille corrigée avec la version 1.0.1g** publiée le 7 avril, jour de l'annonce publique du trou de sécurité. Depuis, entreprises et acteurs concernés s'attachent à combler les trous et (à renforcer la sécurité des futures versions. D'autant que la NSA, l'Agence de sécurité américaine popularisée pour ses méthodes d'espionnage planétaire révélées par Edward Snowden, connaissait l'existence de la faille Open SSL depuis 2 ans et l'a certainement exploitée.

C'est un certain Ivan Kwiatkowski qui, sur le site de discussions d'experts en sécurité Seclists.org, lève le voile. Dans son message, il déclare être entré en contact avec le(s) pirate(s) en question pour leur demander une démonstration sur son propre serveur de l'exploitation de la faille. Le résultat ne s'est pas fait attendre. Selon lui, les données chiffrées susceptibles d'avoir été récupérées et qui lui ont été renvoyées **ont « *de toute évidence* » été « *fabriquées* » de toutes pièces**. « *Si quelqu'un se demande si l'exploit [d'Open SSL] est légitime ou non, maintenant nous savons* », écrit-il dans son post.

Profiter du phénomène médiatique

Au-delà de cette démonstration, **l'attitude du groupe de pirates impliqué est dans tous les cas des plus suspectes aux yeux de Laurent Heslault, directeur technique chez Symantec.** « *On ne poste pas [l'offre de vente d'un exploit] sur Pastbin, une plateforme ouverte, mais sur le darkweb avec une mise en contact en IRC et non par une adresse email* », fait-il remarquer. Par ailleurs, même s'il n'a pas étudié le cas présent en question, les 2,5 Bitcoin réclamés pour le code d'exploitation (autour de 800 euros) représentent selon lui un montant ridiculement bas. « ***Une vraie faille qui permettrait d'obtenir les 64 Ko de données en clair se négocierait plusieurs centaines de milliers d'euros.*** »

Pour lui, et à titre personnel (et non pas celui de Symantec), c'est une arnaque. « *On s'y attend depuis le début. Il y a toujours des petits malins qui tentent de profiter d'un phénomène médiatique et sautent sur l'occasion pour infecter des machines avec des attaques plus traditionnelles.* » A commencer par la récente vulnérabilité Internet Explorer « *plus facile à exploiter [que Heartbleed], plus payante et pas corrigée* ». Sans oublier les 23 failles zero day de 2013 dont 97% de celles qui ont été exploitées

concernaient la plate-forme Java, selon Internet Security Threat Report 2014 de l'éditeur de sécurité.

Il n'en reste pas moins qu'on ne viendra pas pleurer sur le sort des victimes flouées par les pirates arnaqueurs et qui auraient probablement cherché à utiliser l'exploit à des fins malintentionnées…

Lire également

Faille Heartbleed : la check-list pour s'en sortir
La faille Heartbleed exploitée pour attaquer les VPN d'entreprise
Réseau : les matériels Cisco et Juniper touchés par la faille Heartbleed
La faille Heartbleed fait ses premières victimes, dont le fisc canadien