Heartbleed : 2 sites Web sur 3 touchés par la faille OpenSSL ?

Une nouvelle faille majeure frappe Internet. Elle vient d'être révélée par des chercheurs de Google et de l'éditeur en sécurité Codenomicon Defensics. Baptisée Heartbleed, la vulnérabilité référencée CVE-2014-0160 permet à des pirates d'accéder aux informations personnelles (jusqu'à 64 Ko de données) et chiffrées des utilisateurs lors de transactions en ligne.

Le trou de sécurité touche le logiciel OpenSSL chargé de protéger login de connexion, mot de passe, numéro de carte bancaire et autres données depuis le serveur qui héberge la transaction en cryptant la communication réalisée depuis le terminal (PC, tablette, smartphone…) sous protocole SSL/TLS.

Une faille vieille de plus de deux ans

« Le bug Heartbleed permet à n'importe qui sur Internet de lire la mémoire des systèmes protégés par les versions vulnérables du logiciel OpenSSL, indique le site dédié à la faille Heartbleed.com. *Cela compromet les clés secrètes utilisées pour identifier les fournisseurs de services et crypter le trafic, les noms et les mots de passe des utilisateurs et le contenu réel. Cela permet aux attaquants d'espionner les communications, de voler des données directement depuis les services et les [terminaux des] utilisateurs et usurper des services et des utilisateurs. »* On ne peut être plus clair.

Paradoxalement, ce sont les versions les plus récentes du logiciel qui sont affectées : les 1.0.1, 1.0.1f et 1.0.2-beta. Les versions antérieures (1.0.0 et 0.9.8) seraient épargnées. Il n'en reste pas moins que le bug a été introduit en décembre 2011. Voilà donc plus de deux ans qu'il met en danger les communications chiffrées sur Internet (les transactions mais aussi éventuellement les communications par messagerie instantanée et e-mail) et certains réseaux privés virtuels (VPN) généralement souscrits pour les besoins de sécurité des entreprises.

La moitié des sites Web concernés

Selon l'entreprise de sécurité Fox-IT (qui détaille les procédures de test à la vulérabilité), pas moins de la moitié des sites Internet seraient affectés par la vulnérabilité. De fait, OpenSSL est utilisé par les serveurs Apache et nginx qui composent, selon Netcraft, 66% des serveurs web. Néanmoins, l'exploitation de Heartbleed dépend de la façon dont le logiciel est implémenté. Du coup, parmi les géants du Net, seul Yahoo en aurait été victime. Microsoft, Google, Facebook, Apple n'en seraient pas affectés. Pas plus que la majorité des sites bancaires et d'e-commerce.

Il n'en reste pas moins que la mise à jour vers une version corrigée d'Open SSL (la 1.0.1g et prochainement la 1.0.2-beta2) est indispensable pour les sites affectés. Yahoo pour sa part a déclaré avoir résolu le problème. D'autres acteurs, comme CloudFlare, fournisseur de solutions d'optimisation d'applications cloud, ont également anticipé et mis à jour leurs systèmes avant l'annonce publique de la faille lundi 7 avril. Pas de panique, donc. Fox-IT recommande néanmoins

aux administrateurs de renouveler les clés privées de chiffrement et de remplacer les certificats. L'utilisateur, lui, a tout intérêt à changer ses mots de passe après que ses sites d'e-commerce favori ou bancaires ait corrigé le problème.

crédit photo © Sashkin – shutterstock

Lire également
[550 millions de données personnelles dérobées en 2013]