Heartbleed : la faille qui met OpenSSL, et la NSA, sur la sellette

Depuis quelques jours, la faille qui touche le logiciel libre OpenSSL, du nom d'Heartbleed, défraye la chronique. Il est vrai que cet outil est employé pour apporter la **connectivité HTTPS à près de 65 % des sites web** à travers le monde.

Cette affaire a pris une nouvelle ampleur avec les révélations faites par *Bloomberg*, qui indique que l'agence nationale de sécurité américaine, **la NSA, était au courant de l'existence** de cette vulnérabilité depuis deux ans (bref, quasiment depuis son arrivée, en janvier 2012), et l'exploitait afin de capter des transmissions chiffrées, dont la sécurité était compromise par la faille.

La Maison Blanche dément…

« Les rapports indiquant que la NSA ou toute autre partie du gouvernement étaient au courant de la vulnérabilité dite Heartbleed avant avril 2014 ont tort », explique la Maison Blanche dans un communiqué. *« Le gouvernement fédéral n'était pas au courant de la vulnérabilité récemment identifiée dans OpenSSL jusqu'à ce qu'elle ait été rendue publique dans un rapport de cybersécurité en provenance du secteur privé. »*

« Si le gouvernement fédéral, y compris la communauté du renseignement, avait découvert cette vulnérabilité avant la semaine dernière, il l'aurait divulguée aux responsables d'OpenSSL. »

… sous réserve

Le gouvernement américain a indiqué que lorsque la NSA trouvait de telles failles majeures dans les composants de base d'Internet, il était de son devoir de s'assurer qu'elles soient comblées. *« Sauf si la sécurité nationale est en jeu, ou si la faille permet de faciliter l'application de la loi »*, précise également le gouvernement. Déclaration qui contredit tout ce qui a été dit plus haut.

Résumé : les failles de type zero-day découvertes par la NSA doivent être rendues publiques lorsque le pays risque d'en souffrir (rappelons – dans le cas d'Heartbleed – que la plupart des sites gouvernementaux américains utilisent OpenSSL), mais probablement pas dans les autres cas, les États-Unis ayant depuis longtemps élevé le renseignement au rang de cause de sécurité nationale.

Une fondation aux moyens insuffisants

La communauté s'est activée de façon exemplaire depuis la divulgation de cette faille. Ainsi, un correctif a été rapidement fourni. La plupart des sites web d'importance ont maintenant **basculé sous OpenSSL 1.0.1g**, qui élimine ce problème.

Mais, in fine, c'est bien une certaine forme d'échec du modèle open source auprès du public qui transparaît ici. OpenSSL est un composant crucial du web, qui ne soulève toutefois que peu

d’enthousiasme de la part des développeurs.

Conséquence de ce manque d’attractivité, **la fondation OpenSSL travaille avec un budget minimal** et le logiciel est géré par quatre développeurs, dont **un seul employé à temps complet**. Le code incriminé avait ici été inclus dans le projet sans aucun audit… faute de moyens. Du moins aucun audit officiel, les agences de renseignement de la plupart des pays ayant probablement plusieurs dizaines de personnes chargées de trouver des vulnérabilités dans cet outil.

En complément :

– Réseau : les matériels Cisco et Juniper touchés par la faille Heartbleed

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

Voir aussi

– Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales