Faille Heartbleed : le patch d'Akamai était vérolé

Le mouvement de panique engendré par la découverte de la faille Heartbleed, faille touchant le protocole OpenSSL employé par environ deux sites Web sur trois, a-t-il conduit Akamai à agir top vite ? L'entreprise, qui gère environ 30 % du trafic Internet, a reconnu que le bout de logiciel fourni à ses clients pour se prémunir d'Heartbleed contenait un bogue. Ce dernier a été découvert par **un chercheur indépendant en sécurité, Willem Pinckaers**, a reconnu le directeur technique d'Akamai dans un billet de blog.

Cette vulnérabilité pousse Akamai à réémettre tous les certificats SSL et les clefs de sécurité assurant les connexions cryptées entre les sites de ses clients et les internautes. La société américaine fait tourner 147 000 serveurs dans 92 pays. Elle est l'une des nombreuses sociétés à avoir recours à la librairie open source de cryptage OpenSSL.

Rappelons que la faille Heartbleed résulte d'une erreur de programmation d'un développeur allemand voici deux ans. Cette erreur permet notamment, si elle est exploitée, à un assaillant de **récupérer la clef privée utilisée pour créer une connexion SSL**.

Patch bourré de bogues

Après divulgation de l'existence d'Heartbleed, Akamai avait expliqué que son implémentation de OpenSSL était moins fragile que d'autres, en raison d'un **code propriétaire** modifiant la façon dont les clefs de cryptage sont stockées. Ce qui n'avait pas empêché la société de le modifier, créant une variante censée sécuriser davantage les clefs privées. C'est cette variante qui s'est révélée défectueuse.

A la décharge d'Akamai, en fin de semaine dernière, la société ne présentait son code modifié que comme un prototype ne devant pas être mis en production tel quel. « *Peut-être Akamai ne fait actuellement pas tourner cette version en production, mais un autre outil d'allocation mémoire 'super-sécurisé'. Quoi qu'il en soit, la société ne devrait pas soumettre à la communauté OpenSSL des patch non fonctionnels et bourrés de bogues, tout en affirmant que ces dernier protègent Akamai de l'attaque Heartbleed* », assure Willem Pinckaers, qui affirme que l'analyse du code lui a pris… 15 minutes.

Le fait que la société ait pris le parti de **réémettre tous les certificats utilisés par ses plates-formes** montre que la démonstration de Willem Pinckaers doit avoir une certaine portée. Et concerne, probablement, le code d'implémentation avant même la publication de la variante de la fin de la semaine dernière.

En complément :

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

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