Google va payer les développeurs améliorant la sécurité des logiciels open source

En matière de sécurité, **Google** fait le maximum pour que les failles soient découvertes et comblées en toute transparence. Afin de limiter (casser ?) le marché des failles zero day, la firme rétribue en effet les personnes découvrant des vulnérabilités dans ses services web, et son navigateur web Chrome.

Google étend aujourd'hui ce service à un large ensemble de logiciels open source.

« Nous bénéficions tous de l'incroyable travail bénévole accompli par la communauté open source. C'est pourquoi nous continuons à nous demander comment allier ce modèle de développement à notre Vulnerability Reward Program*, afin d'améliorer la sécurité des logiciels essentiels à la santé de l'ensemble d'Internet, »* explique **Michal Zalewski** de la Google Security Team, sur le blogue sécurité de la firme.

Plutôt que de payer les chercheurs corrigeant des failles de sécurité dans les logiciels open source, Google a opté pour un modèle différent : rétribuer les développeurs effectuant des changements dans du code open source afin d'en améliorer le niveau de sécurité.

Un programme en deux étapes

Google va donc verser de l'argent aux personnes améliorant la sécurité certains de composants clés du monde open source. Seront initialement concernés les produits suivants :

- Services d'infrastructure réseau : OpenSSH, BIND, ISC DHCP ;
- Outils de traitement d'images : libjpeg, libjpeg-turbo, libpng, giflib ;
- Fondations de Google Chrome : Chromium, Blink ;
- Autres librairies : OpenSSL, zlib ;
- Composants critiques du noyau Linux (y compris KVM).

Cette première vague servira en partie les intérêts de Google, ces composants étant en majeure partie utilisés au sein de Chrome et de Chrome OS.

Dans un second temps, le programme sera étendu aux composants open source suivants :

- Serveurs web : Apache httpd, lighttpd, nginx ;
- Services SMTP : Sendmail, Postfix, Exim ;
- Outils de développement : GCC, binutils, llvm ;
- Virtual private networking : OpenVPN.

Le modèle de rétribution reste classique (par rapport aux programmes de découverte de failles de Google), avec le versement de primes allant de 500 dollars à 3133,7 dollars pour les correctifs retenus.

Voir aussi

Quiz Silicon.fr – 10 questions sur Google