Open Source : Google complète son programme Patch Rewards

Google a annoncé mercredi réorganiser son Patch Rewards Program. Le programme a été lancé en octobre 2013 pour récompenser les chasseurs de failles et l'apport de correctifs dans certains projets open source. À l'origine, Google s'engageait à soutenir les améliorations de sécurité apportées à ces projets, une fois implémentées les fonctionnalités en question.

Le programme évolue. À partir du 1er janvier 2020, Google « apportera également un soutien financier initial [aux projets sélectionnés] pour fournir aux développeurs open source une ressource supplémentaire permettant de prioriser le travail de sécurité », a indiqué dans un billet de blog Jan Keller, responsable de programme technique sécurité chez Google.

Deux niveaux d'incitation seront proposés : l'un à 5000 dollars, pour soutenir la résolution d'un petit nombre de problèmes de sécurité, y compris en appportant un correctif de failles identifiées lors d'un bug bounty, l'autre à 30 000 dollars pour « inciter un projet plus important à investir massivement dans la sécurité. »

Les soumissions de projets seront examinées chaque mois en vue d'un éventuel financement. « Lors de la sélection, le panel mettra l'accent sur les projets essentiels à la santé d'Internet ou sur les projets d'utilisateurs finaux avec une large base [d'internautes] », a ajouté Jan Keller.

Au-delà du Bug Bounty

Les évolutions annoncées viennent s'ajouter au programme Patch Rewards existant.

Les projets open source concernés par le programme, jusqu'ici, sont :

– Chromium, Blink, Omaha, AOSP
– Linux kernel (dont KVM)
– Apache httpd, lighttpd, nginx, Sendmail, Postfix, Exim, Dovecot
– OpenSSH, OpenVPN, BIND, ISC DHCP, University of Delaware NTPD
– libjpeg, libjpeg-turbo, libpng, giflib, zlib, libxml2
– OpenSSL, Mozilla NSS
– Google projet Certificate Transparency
– outils de sécurité pour GCC, binutils et llvm
– yum, apt, pip, npm
– Angular, Closure, Dart, Django, Dojo Foundation, Ember, GWT, Go, Jinja (Werkzeug, Flask), jQuery, Knockout, Polymer, Struts, Web2py, Wicket
– zlib, bzip2, tar, gzip, info-zip, cpio, xz, 7z, p7zip, ncompress, lzo
– logiciel critique utilisé pour le cloud : le proxy Envoy
– OSS-Fuzz

« Tout correctif ayant un impact démontrable, significatif et proactif sur la sécurité de l'un des projets concernés sera considéré pour une récompense », a insisté Google.

crédit photo © Shutterstock