Bug Bounty : GitHub a versé plus de 166 000 dollars en 2017

Après avoir été la cible d'une attaque majeure par déni de service distribué (DDoS) le 28 février, la plateforme de développement logiciel GitHub fête le quatrième anniversaire de son programme Bug Bounty.

La participation de chercheurs en sécurité ayant découvert des vulnérabilités, les initiatives lancées et les primes versées ont toutes augmenté ces dernières années.

En 2017, 840 propositions ont été examinées et triées. 121 découvertes de vulnérabilités ont été jugées valides (contre 48 sur 795 en 2016). Elles ont été résolues et les chercheurs récompensés. Le total des sommes versées est passé de 95 300 dollars en 2016 à 166 495 dollars en 2017 (soit un paiement moyen de 1 376 dollars).

Cette croissance s'explique par l'augmentation des rapports valides. Mais aussi par la réévaluation des primes pour s'aligner sur le concours Hack the World de HackerOne. Par ailleurs, le référentiel GitHub Enterprise a été ajouté au périmètre du programme.

Protéger l'écosystème GitHub

GitHub veut être en phase avec *« les meilleurs »* concours de chasse aux failles de sécurité. Des concours que pratiquent Google, Facebook, Mozilla et bien d'autres entreprises.

Pour 2018, la plateforme indique dans un billet de blog lancer *« davantage de primes privées et de bourses de recherche »*. GitHub réfléchit également à une extension du programme pour sécuriser plus avant ses services de production et mieux protéger son écosystème.

Lire également :

GitHub alerte les développeurs des vulnérabilités dans leur code

GitHub dévoile la face cachée du développement Open Source

(crédit photo © Vchal-Shutterstock)