Bug Bounty : GitHub augmente ses primes de chasse aux bugs

La plateforme de partage de code GitHub renforce son programme et ses primes de chasse aux bugs informatiques initiés en 2014.

Son programme de bug bounty couvre désormais tous les services de premier plan hébergés sous le domaine github.com, à savoir : GitHub Education, GitHub Learning Lab, GitHub Jobs et GitHub Desktop.

GitHub Enterprise Cloud (GitHub Enterprise Server est lui couvert depuis 2016) et l'ensemble des services de premier plan associés aux domaines githubapp.com et github.net sont également couverts.

Dans ce contexte, les primes ont été révisées à la hausse.

Supprimer le plafond

L'entreprise veut adapter son programme au marché. Et récompenser le fait qu'il est plus difficile que par le passé de détecter des vulnérabilités critiques dans les produits GitHub.

Les montants varient en fonction du niveau de criticité des vulnérabilités :

– Critique : entre 20 000 et plus de 30 000 dollars (le plafond a été supprimé) ;
– Haut : entre 10 000 et 20 000 dollars ;
– Moyen : de 4 000 à 10 000 dollars ;
– Faible : entre 617 et 2 000 dollars.

Pour les découvertes de failles jugées les plus critiques, l'entreprise détenue par Microsoft a indiqué « se réserver le droit d'augmenter considérablement les montants versés ».

250 000 dollars versés en 2018

En 2018, plus de 250 000 dollars ont été alloués aux chercheurs en sécurité via différentes actions (programmes privé – lié à GitHub Actions – et public de bug bounty, bourses et événement hacker H1-702 porté par HackerOne).

Notons que sur les 250 000 dollars annoncés, 165 000 dollars ont été octroyés dans le cadre du seul programme public de chasse aux bugs de GitHub. Un montant stable par rapport à celui de 2017 (le paiement moyen d'une découverte valide était de 1 376 dollars).

En plus d'augmenter les primes, l'entreprise a annoncé dans son billet de blog mieux protéger les participants au programme des risques juridiques liés à la recherche de failles de sécurité. Dans ce but, GitHub a ajouté à sa politique des conditions légales de type Safe Harbor (sphère de sécurité), sur la base des modèles de licence CC0.

(crédit photo © GitHub)