HackerOne ouvre ses Bug Bounties aux projets Open Source

Depuis l'affaire Heartbleed, la sécurité des projets Open Source fait couler beaucoup d'encre. Plusieurs acteurs IT et non des moindres, comme Google, Facebook et Microsoft, avaient alors lancé le projet Core Infrastructure Initiative pour soutenir les travaux sur la sécurité des projets Open Source.

Mais cette initiative n'empêche pas pour autant de découvrir des failles dans différents services Open Source. Y compris longtemps après leur sortie. Pour apporter sa pierre, HackerOne, plateforme de recherche de bug, vient de lancer une offre Community Edition, gratuite, à destination de ces solutions. Cette proposition est identique à l'édition professionnelle à destination des grandes entreprises clientes de la plate-forme, comme Twitter, Dropbox, Adobe, Yahoo, Uber, GitHub, Snapchat, etc., sauf qu'elle n'offre pas d'assistance dédiée.

Quelques critères à respecter

Pour prétendre à un bug bounty gratuit sur HackerOne, les projets doivent remplir quelques critères. Ils doivent être actifs et afficher au moins 3 mois d'existence (au regard des livrables et des contributions au code) ; ils doivent fonctionner sous une licence compatible OSI ; ils doivent être prêts à ajouter un fichier security.md à la racine de leur projet ; ils doivent afficher un lien vers le bug bounty HackerOne sur la page d'accueil du projet ou dans le menu de navigation et, enfin, ils doivent s'engager à répondre aux tickets de sécurité dans un délai d'une semaine.

Il n'y a par contre aucune limite, ni aucun critère relatif à la popularité du projet. Ainsi, n'importe quel service peut soumissionner, depuis les plugins jQuery jusqu'aux CRM les plus complexes et aux plateformes de e-commerce. HackerOne indique que plusieurs solutions Open Source l'ont déjà rejoint, avant même l'annonce de l'édition communautaire. Et de citer Django, Discourse, Ruby, Ruby on Rails, Brave, GitLab et Sentry.

50 ingénieurs de Google sauvent des projets de Mad Gadget

Cette démarche intervient au moment où Google vient de lever sur le voile sur une opération nommée Rosehub qui a mobilisé 50 de ses ingénieurs pendant 2 ans. Ces professionnels ont pris sur leur temps de travail pour corriger une faille critique dans Java qui touchait plusieurs milliers de projets Open Source. Cette vulnérabilité, connue sous le nom Mad Gadget en interne, a été découverte au début 2015 et a commencé à faire parler d'elle à la fin de cette même année. Cette faille a été utilisée notamment dans le cadre du piratage par un ransomware de la société des transports en commun de San Francisco.

A lire aussi :

Le Bug Bounty de l’US Army trouve une faiblesse du réseau interne

Hack le Pentagone : déjà 100 bugs découverts

Crédit photo : GlebStock / Shutterstock