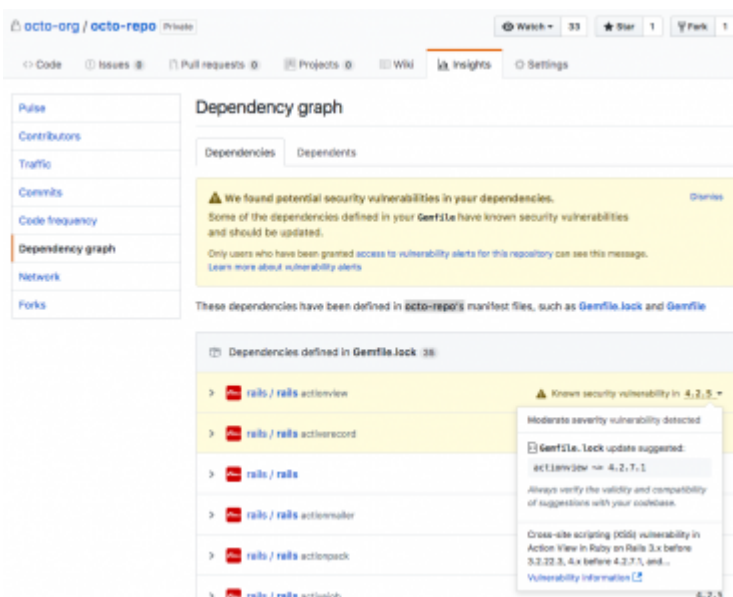


GitHub alerte les développeurs des vulnérabilités dans leur code

GitHub entend renforcer la sécurité des projets soumis par les **développeurs**.

La plate-forme de partage de codes informatiques annonce une nouvelle fonctionnalité visant à alerter les développeurs quand ces derniers utilisent des briques Open Source entachées d'une vulnérabilité de sécurité.

« Avec votre graphique de dépendances activé, nous vous avertirons désormais lorsque nous détectons une vulnérabilité dans l'une de vos dépendances et suggérons des correctifs connus de la communauté GitHub », annonce la plate-forme sur son [blog](#).



Cette nouvelle fonctionnalité, « alerte de sécurité », entend s'adresser aux 75% de projets de la plate-forme développés avec des briques de codes Open Source.

Cette veille de sécurité s'inscrit dans la continuité de l'offre de « graphe de dépendance » (Dependency Graph) lancée le mois dernier et qui permet aux développeurs de suivre les évolutions des dépendances sur lesquelles s'appuient leurs programmes.

Pour l'heure, seuls les langages JavaScript (fichiers package.json) et Ruby (gemfiles) sont supportés. Python le sera courant 2018.

Les CVE et les autres

Si les vulnérabilités référencées auprès de la National Vulnerability Database sous forme de CVE (Common Vulnerabilities and Exposures) seront par défaut intégrées aux alertes de sécurité, GitHub n'entend cependant pas négliger les failles non référencées. D'autant que nombre d'entre elles peuvent être publiquement exploitées.

« Nous continuerons d'améliorer l'identification des vulnérabilités à mesure que nos données de sécurité croîtront », souligne la plate-forme de référence de partage de codes. Tout en invitant les développeurs à se tourner vers les partenaires en sécurité Snyk et Gemnasium.

Les alertes de sécurité sont disponibles à travers la plate-forme et s'active quand le développeur utilise une bibliothèque affectée par une vulnérabilité. Mais aussi par e-mail.

Le graphique de dépendances enverra des notifications par courriel chaque fois qu'un projet est mis à jour avec l'utilisation d'une dépendance vulnérable.

Ou encore quand GitHub met à jour sa base de données propre aux vulnérabilités. Autant de services qui devraient aider à renforcer la sécurité des applications.

Lire également

[Près de 9 applications Java sur 10 vulnérables](#)

[Les sites web menacés par les bibliothèques JavaScript obsolètes](#)

[Une faille Apache Struts menace 65% des entreprises du Fortune 100](#)

Crédit Photo : Smeisatch-Shutterstock