Sécurité : Microsoft automatise la recherche de bugs

Microsoft met en ligne son outil de détection de failles de sécurité, Security Risk Detection (SRD). Ce dernier est censé mettre au jour les failles avant que celles-ci ne soient officiellement découvertes, afin de faciliter leur correction à la fin de l'étape de développement. SRD est disponible pour Windows et pour Linux, dans une version préliminaire. Annoncé en septembre dernier et connu sous l'appellation de projet Springfield, l'outil automatise le fuzzing, une technique de tests automatiques consistant à fournir des données invalides, non prévues ou aléatoires à des programmes, afin de détecter des crashs ou autres erreurs comme des corruptions de mémoire. Ce qui permet aux développeurs de détecter des problèmes dans leurs applicatifs avant de les mettre en production.

Après s'être identifiés sur un portail web, les utilisateurs de SRD pourront installer les binaires du programme au sein d'une machine virtuelle, ainsi qu'un gestionnaire qui va lancer les scénarios de tests et échantillonner les fichiers qui vont servir à éprouver la robustesse du programme cible. SRD exploite également des mécanismes d'IA pour automatiser les processus de raisonnement amenant habituellement les experts en sécurité à découvrir les zones de fragilité d'un logiciel. L'outil exploite le Cloud pour partager l'expérience de ses utilisateurs et entraîner ses algorithmes.

Faire face à pénurie d'experts en sécurité

Le service a été conçu pour les organisations qui écrivent leur propre logiciel, modifient des programmes du commerce ou exploitent sous licence des offres Open Source. SRD ne nécessite pas l'accès au code source, explique David Molnar, chercheur principal et chef de projet chez Microsoft. Les utilisateurs peuvent y injecter n'importe quel logiciel Open Source.

SRD repose sur deux avancées, selon Molnar. Primo, le débogage historisé, qui permet aux utilisateurs de revenir sur leur logiciel pour voir où et quand des défauts y ont été introduits. Secundo, la technique dite de résolution de contraintes (où la relation entre des variables est établie sous forme de contraintes) appliquée à la chasse aux bugs, le sujet de recherche de David Molnar.

« Nous pensons que SRD peut aider à faire face à la pénurie de professionnels de la sécurité en facilitant le travail des développeurs sans expérience sur ce sujet », explique Molnar. Microsoft envisage de rendre le service payant plus tard dans le courant de l'été.

A lire aussi :

Open Source : avec OSS-Fuzz, Google paye les développeurs qui testent leurs projets

L'Open Source fait peser des risques sur la sécurité de l'entreprise

HackerOne ouvre ses Bug Bounties aux projets Open Source

Crédit photo © andriano.cz – shutterstock