Dompter le monstre Open Source avec une solution efficace de tests de la sécurité des applications

4 mai 2017 | Par David Marshak

Impact des attaques sur l'efficacité de vos tests de sécurité des applications

Et cela recommence : une nouvelle attaque avec un nom bizarre va bientôt faire la une des journaux ! Plus dangereuse que Ghost, POODLE, FREAK, Heartbleed, Shellshock ou que les 6 000+ attaques comptabilisées chaque année, et nous ne savons actuellement que deux choses sur elle :

1. Elle ciblera probablement un composant open source vulnérable.
2. Il est extrêmement probable que ce composant open source est présent dans vos applis.

Le challenge de l'open source

Devriez-vous demander à vos développeurs de ne plus utiliser l'open source ? Mais ce n'est pas possible sans nuire à leur productivité. De plus, les logiciels n'ont jamais autant utilisé de composants open source qu'aujourd'hui. Dans son rapport « Secure Applications at the Speed of DevOps », Forrester indique qu'environ 80 à 90 % du code des applications modernes proviennent de composants open source.

Il est évident que l'open source est là pour rester. Pour vous protéger, vous devez tester proactivement votre code pour être certain qu'aucune de vos bibliothèques n'est vulnérable. Et comme il est probable que votre entreprise soit vulnérable d'une façon ou d'une autre, vous devez vous concentrer sur deux facteurs de réussite spécifiques.

Facteur de réussite No.1 : Intégrer les tests Open Source dans la démarche DevOps

Le plus important pour vous est de connaître les packages open source que vos développeurs utilisent et identifier tout particulièrement ceux qui contiennent des vulnérabilités exploitables. Il est indispensable que cette évaluation soit effectuée le plus tôt possible pendant le cycle de développement et qu'elle soit continue, puisque les menaces changent constamment.

Forrester recommande en particulier d' : ‘ Intégrer le plus tôt possible un outil d'analyse de composition logicielle (SCA) dans le SDLC et de continuer à scanner les applications, en incluant les applications antérieures dont les cycles d'actualisation sont longs ou erratiques, pour débusquer les vulnérabilités plus récentes. La meilleure solution consiste à intégrer la découverte open source directement dans les tests de sécurité des applications en cours, pour qu'ils deviennent inséparables de votre stratégie DevOps.

Avec IBM®, ce processus est facile et transparent. Depuis le lancement d'IBM Application Security Open Source Analyser, qui fait partie d'IBM Application Security on Cloud, l'identification des composants open source est automatique pendant les tests des applications (SAST). Ces composants sont comparés à une liste de vulnérabilités connues. Les résultats de cette comparaison sont non seulement exploitables, mais ils incluent aussi des recommandations spécifiques, telles que le remplacement de certains composants par des versions plus récentes. Les résultats sont directement intégrés dans des rapports d'identification et de correction des vulnérabilités détectées dans votre code. Ils favorisent l'adoption et l'utilisation transparentes de modèles qui joueront un rôle décisif dans votre réussite.