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

Les applications Open Source sont-elles plus dangereuses pour la sécurité des entreprises que les solutions propriétaires ? Le Centre de recherche et d’innovation Open Source (Cosri pour *Center for Open Source Research & Innovation*) de l’éditeur Black Duck Software s’est penché sur cette question qui, pour des raisons plus ou moins légitimes, oppose de manière récurrente les tenants du libre aux inconditionnels du modèle fermé. Plus que de vouloir opposer deux modèles de licences, le Cosri cherche avant tout à aider les organisations à mieux appréhender le modèle Open Source afin qu’elles améliorent leurs processus de gestion de risques applicatifs… notamment à travers les solutions que propose Black Duck spécialisé dans la gestion du risque Open Source.

Du millier (1 071 précisément) d’applications commerciales auditées en 2016 par le Cosri, notamment dans le cadre d’opérations de fusion-acquisition, il ressort que 96% d’entre elles embarquent des composants Open Source. A raison de 147 par application en moyenne. Autant dire que le libre est aujourd’hui partout dans l’entreprise. Ce qui n’est pas sans poser problème alors que des vulnérabilités touchent 67% des applications open source analysées, selon l’étude annuelle de Black Duck. Avec 27 brèches de sécurité par application en moyenne. Un taux en hausse en regard des 22,5 constatées en 2015. Plus inquiétant encore, les vulnérabilités identifiées sur les applications auditées ont plus de 4 ans en moyenne (1 527 jours). Et plus de 5 ans pour 67% des codes étudiés.

Problèmes de licences

Autre fait préoccupant, la mauvaise gestion des licences pourrait être dommageable pour les organisations alors que 85% des applications scrutées par le Cosri contiennent des composants avec des licences non conformes. Autrement dit, marqués par des conflits portant sur des violations de licences GPL la plupart du temps. Et 53% ne disposent carrément pas de licences clairement identifiées. L’entreprise se retrouve ainsi dépourvue d’autorisation pour modifier et redistribuer le code. Avec le risque d’un futur conflit en regard d’une exploitation potentiellement illégale du composant.

Les secteurs de la grande distribution et du commerce en ligne sont particulièrement touchés par le phénomène. 83% de leurs applications auditées contiennent des failles de sécurité hautement élevées. Suivi par les acteurs de l’Internet et des logiciels d’infrastructure à hauteur de 70%. Les services financiers se montrent également concernés avec 60% d’applications hautement vulnérables. A peine plus que le Big Data/AI/BI/Machine Learning, ainsi que la cybersécurité ou encore l’Industrie/Robotique affectés à hauteur de 59% chacun.

Des vulnérabilités dans les composants populaires

Nombre de ces vulnérabilités se concentrent parmi les composants Open Source les plus populaires comme Open SSL, Apache Tomcast ou Apache Struts présents dans 8,3%, 10,1% et 3,9%

des applications analysées. A lui seul, les modules Open SSL étudiées renfermaient 27 vulnérabilités en moyenne, contre 20 pour Apache Struts et 11 pour Apache Tomcast. L'audit de Black Dusk révèle que 52,6% des vulnérabilités trouvées sont classées comme «élevées» (high) par le National Institute of Standards and Technology (NIST).

De fait, l'insécurité ne vient pas nécessairement du développement des applications Open Source dont le modèle permet d'accélérer l'innovation et la mise sur le marché des produits, mais de la façon dont les entreprises gèrent leurs logiciels. Elles doivent notamment assurer le suivi de veille des mises à jour des composants en regard de la publication de nouvelles versions. Et cela d'autant que les vulnérabilités sont dévoilées publiquement.

« Avec 3623 nouvelles vulnérabilités des composants open source signalées en 2016 - près de 10 par jour en moyenne et une augmentation de 10% par rapport à l'année dernière - le besoin de sécurisation et d'une gestion Open Source efficaces est plus important que jamais, souligne le rapport disponible à partir de cette page. *La détection et l'assainissement des vulnérabilités de sécurité devraient être une priorité absolue. »*

Lire également
Sécurité : l'Europe inclut un bug bounty à son audit logiciel
Open Source ou propriétaire ? Les entreprises font le choix de la mixité
Le code des logiciels propriétaires plus conforme que l'Open Source

crédit photo © Zothen – Fotolia.com