Open source : des facteurs limitants pour les applications d'entreprise

L'*open source* n'est pas épargné par la problématique des systèmes hérités.

La Fondation Linux en est arrivée à ce constat à l'issue d'une étude menée avec l'université de Harvard.
Des spécialistes de l'analyse logicielle et de la sécurité applicative ont été sollicités dans ce cadre. Ils ont fourni des données issues d'audits de bases de code et de scans automatisés d'environnements de production chez leurs clients.

Le rapport qui en ressort met en lumière d'autres facteurs potentiellement limitants associés à l'usage de l'*open source* dans les applications d'entreprise.

L'absence d'un nommage standardisé pour les composants logiciels est un de ces facteurs. Elle est susceptible de compliquer le partage d'informations dans le cadre des stratégies de transparence et de sécurité.
Le problème n'est pas nouveau. La Fondation Linux l'avait déjà rencontré en 2015 lors d'une étude visant à identifier les composantes les plus critiques de Debian.

Tendance *legacy*

La réalité du *legacy* transparaît dans la liste des paquets logiciels les plus utilisés sur l'échantillon analysé. En particulier avec le module minimist, plus populaire que yargs, pourtant censé lui avoir succédé.

À quoi est due cette résilience de composants obsolètes ou plus mis à jour depuis des années ? La Fondation Linux est partagée. D'un côté, elle déplore la faible valeur ajoutée que perçoivent les organisations en rapport aux coûts induits. De l'autre, elle reconnaît qu'il faudrait approfondir la réflexion, pour déterminer si le *legacy* est véritablement exploité ou s'il est simplement conservé à des fins de tests de caractérisation.

Autre écueil : l'utilisation massive de comptes individuels.
7 des 10 paquets logiciels les plus utilisés étaient, au moment de l'analyse, hébergés sur ce type de compte, qui propose de manière générale moins d'options de protection que les comptes d'organisations.

Cette situation a été mise à profit en 2016 pour intégrer une *backdoor* dans la bibliothèque JavaScript event-stream. Elle l'a été plus récemment (été 2019) pour attaquer le dépôt officiel RubyGems.

La dépendance vis-à-vis de comptes individuels pose d'autres risques, illustrés en 2016. Un développeur, accusé de violation de marque, avait cassé des milliers de projets en supprimant du gestionnaire npm le module left-pad.

En toile de fond, un autre rapport publié cette semaine, et signé Red Hat. L'éditeur qui évolue désormais dans le giron d'IBM affirme que la part de l'*open source* dans les parcs logiciels continue de progresser. Et qu'il devrait en être ainsi au moins pour les deux prochaines années.

Photo d'illustration © opensourceway via*Visual Hunt / CC BY-SA*