Applications : l'obsolescence ignorée de composants open source

Synopsys, éditeur de logiciels de conception et de vérification de circuits intégrés, a réalisé l'audit du codebase (soit l'ensemble du code source utilisé pour un logiciel) d'applications commerciales pour son rapport 2020 (*Open Source Security and Risk Analysis Report*).

Presque tous ces codebases (99%) contiennent au moins un composant logiciel open source. Par ailleurs, 70% de l'ensemble du code analysé est open source. Un doublement en cinq ans.

Seulement, l'utilisation de composants open source obsolètes persiste. 91% des codebases scrutés incluent des composants logiciels dépassés de plus de quatre ans ou qui n'ont pas fait l'objet de développement au cours des deux dernières années, selon le rapport.

L'exposition aux failles de sécurité augmente et les mises à jour peuvent être compliquées par des problèmes de fonctionnalité ou de compatibilité.

Mises à jour, licences et dépendances

Plus préoccupant encore, 75% du codebase étudié contient des composants open source présentant des failles de sécurité connues. Un taux en hausse de 15 points en un an.

De même, près de la moitié (49%) de ce code intègre des vulnérabilités à haut risque, contre 40% déjà 12 mois auparavant. Enfin, des problèmes de licences open source perdurent pour 68% des codebases étudiés.

« Il est difficile d'ignorer le rôle essentiel que joue l'open source dans le développement et le déploiement de logiciels aujourd'hui. Mais il est facile d'ignorer comment il impacte le profil de risque associé à une application en termes de sécurité et de conformité des licences », a déclaré Tim Mackey, stratège en sécurité du Synopsys Cybersecurity Research Center.

Synopsys recommande donc aux entreprises de gérer le risque. « Le maintien d'un inventaire précis des composants logiciels tiers, y compris les dépendances open source, et leur mise à jour, est un point de départ clé pour répondre au risque applicatif sur plusieurs niveaux. »

(crédit photo : via pexels)