Bibliothèques Open Source : des mises à jour qui se font attendre

Le niveau de sécurité de bibliothèques (*libraries*) open source présentes dans 86 000 applications a été analysé. Aussi, près de 2 000 développeurs ont été interrogés dans le cadre du rapport* 2021 sur l'état de la sécurité logicielle – édition open source.

Présentes dans pratiquement toutes les applications, les bibliothèques open source tierces permettent aux développeurs d'y ajouter des fonctionnalités de base.

52% des développeurs interrogés disposent d'un processus formel de sélection des bibliothèques tierces. 28,4% l'ignorent et 19,1% répondent par la négative.

Dans ce contexte, 79% des bibliothèques tierces ne sont jamais mises à jour par les développeurs après avoir été intégrées dans une base de code. Elles sont ainsi davantage exposées à différentes menaces : exécution de code arbitraire, déni de service (DoS), attaques XXE (eXternal XML entities), failles XSS (Cross-site scripting), etc.

« Les bibliothèques open source évoluent constamment, de sorte que ce qui semble sûr aujourd'hui peut ne plus l'être demain », relèvent les auteurs du rapport.

Inventaire et mise à jour logicielle

Lorsque les développeurs sont alertés de la présence d'une bibliothèque vulnérable, ils réagissent plus ou moins rapidement. Ainsi, 17% des bibliothèques vulnérables sont corrigées dans l'heure qui suit l'analyse ayant alerté le professionnel de la faille, 25% dans les sept jours, 50% dans les trois mois…

Pour mieux faire, Veracode recommande de maintenir un inventaire précis des composants logiciels tiers, y compris les dépendances open source et leur mise à jour.

Le fournisseur de solutions de sécurité applicative (AppSec) insiste : 92% des failles des bibliothèques open source pourraient être corrigées par une simple mise à jour. Dans 69% des cas, il s'agit de changements « mineurs » de version.

* Veracode – « State of Software Security (SOSS) vol. 11: Open Source Edition »