Les développeurs victimes des compilateurs effaceurs de code

Les développeurs doivent redoubler de vigilance sur les bugs dans leurs applications. Si on connaît les failles de sécurité ou bug classique, d'autres éléments viennent se greffer comme l'a rappelé une intervention de l'équipe du MIT dirigée par Xi Wang lors de la conférence Usenix qui vient de se dérouler à Philadelphie. Parmi ces autres risques, il se focalise sur celui baptisé « **optimisation de code instable** » ou « **code instable** ». Il provient de la façon dont **un compilateur efface une partie du code sans avertir le développeur**, souligne nos confrères d'IT World. Avec ce code instable, les programmeurs peuvent perdre des fonctionnalités importantes touchant au contrôle de sécurité sans qu'ils le sachent.

Un module d'analyse du code instable

Pour trouver ce code instable dans les programmes écrits en **C++ et C**, l'équipe de scientifiques a développé une technique nommée Stack. Ce produit a été testé et a permis de découvrir **plus de 160 erreurs** dans différentes applications liées au code instable. Dans le détail, 11 bugs ont été trouvés et corrigés dans le protocole d'authentification réseau Open Source Kerberos. De même, 68 bugs ont été recensés par Stack dans le logiciel de gestion de la base de données PostgreSQL ce qui a permis d'appliquer 29 correctifs au sein de la base de données, elle-même. Au final, **la recherche a porté sur 16 compilateurs C/C++ Open Source et propriétaires** de sociétés comme Intel, IBM ou Microsoft. Et le résultat montre que tous laissent passer du code instable.

En complément de la Core Initiative Infrastucture

Avec leur projet Stack, les chercheurs du MIT espèrent **le voir intégrer les compilateurs** pour pouvoir proposer une amélioration du code. Cette démarche n'est pas la seule pour optimiser et sécuriser le code. Après la faille Heartbleed, il y a eu une prise de conscience des grands acteurs du web sur certains projets Open Source critiques. Sous la houlette de la Fondation Linux, Google, Facebook, Microsoft et d'autres travaillent et financent, au sein de la Core Initiative Infrastructure, des audits sur la validité et la sécurité du code de projets comme OpenSSL par exemple.

A lire aussi :

Codecademy : mais alors, you code in French !

La NSA publie des messages codés sur Twitter pour recruter