Près de 9 applications Java sur 10 vulnérables

Selon le State of Software Security (SOSS) 2017 de Veracode, 88% des applications contiennent un ou plusieurs composants vulnérables. Et plus de 53% des applications Java s'appuient sur une version vulnérable des composants issus des collections communes (Commons Collections components).

Ce phénomène s'explique par la réutilisation fréquente de composants Java. Une méthode qui facilite et accélère le développement d'une application. Jusqu'à 75% d'une application peut ainsi être construite à base de composants Open Source, avance le fournisseur de sécurisation du code. Or, il n'est pas rare qu'un développeur ne mette pas à jour son code lorsqu'une faille y est découverte ou quand de nouvelles versions des composants sont disponibles.

Un seul exploit pour des milliers d'applications

« L'utilisation universelle des composants dans le développement d'applications signifie que lorsqu'une seule vulnérabilité dans un seul composant est divulguée, cette vulnérabilité a maintenant le potentiel d'avoir un impact sur des milliers d'applications – ce qui rend bon nombre d'entre elles cassables avec un seul exploit », souligne Chris Wysopal, CTO de la société acquise par CA Technologies en mars.

Et de citer l'exemple de la faille « Struts-Shock ». Pas moins de 68% des applications Java s'appuyant sur la bibliothèque Apache Struts 2 utilisaient une version boguée du code. Résultat, 35 millions de sites web étaient vulnérables. D'autant que le correctif contenait lui-même des défaillances.

250 milliards de lignes de code analysées

La 8e édition du rapport de Veracode s'appuie sur 400□000 analyses de code, soit 250 milliards de lignes passées au crible sur 12 mois. Une analyse qui a révélé 12,8 millions de vulnérabilités. L'étude rapporte aussi que seules 28% des entreprises effectuent une analyse pour suivre et surveiller les composantes de leurs applications.

Pas question pour autant de cesser d'utiliser les composants Open Source. Mais il convient de s'assurer de leur intégrité avant de les exploiter. *« Nous avons maintenant constaté un certain nombre de violations en raison de composants vulnérables et, à moins que les entreprises ne commencent à prendre cette menace plus au sérieux, et d'utiliser des outils pour surveiller l'utilisation des composants, je prévois que le problème va s'intensifier »*, alerte Chris Wysopal.

Lire également
Une faille Apache Struts menace 65% des entreprises du Fortune 100
Les sites web menacés par les librairies JavaScript obsolètes