Une faille Java met les applications SAP à découvert

Le moteur J2EE (Java 2 Platform Enterprise Edition) est victime d'un bug qui met en danger l'application NetWeaver de SAP, a révélé le directeur en sécurité **Alexander Polyakov** de la société ERPscan à l'occasion de la conférence Black Hat la semaine dernière. Selon lui, **la moitié des systèmes SAP accessibles depuis Internet peuvent être piratés**. NetWeaver est la plate-forme d'intégration des applications SAP. Lesquelles vont des ERP (PGI) au CRM (GRC) en passant par mySAP Business Suite en passant par les SCM (Supply Chain Management) et PLM (Product Lyfecycle Management). NetWeaver est donc un pilier central des solutions et développements d'applications SAP.

La faille de sécurité est d'autant plus dangereuse qu'elle permet de contourner les mécanisme d'authentification de l'utilisateur. *« Par exemple, il est possible de **créer un utilisateur et l'assigner au groupe des administrateurs** utilisant deux demandes non autorisées au système*, explique ERPscan. *Il est également dangereux parce que l'attaque est possible sur les systèmes protégés par les systèmes d'authentification à deux facteurs, dans lequel il est nécessaire de connaître la clé secrète et le mot de passe pour y accéder. »*

Une faille qui risque donc de permettre aux attaquants de pénétrer les systèmes d'information de plus de **100.000 entreprises dans le monde** dont les principales organisations du classement Fortune 500. Pour palier ce risque, SAP a promis de fournir un correctif rapidement. *« SAP travaille en étroite collaboration avec Alexander Polyakov sur ce problème »*, a commenté l'entreprise. Néanmoins, le correctif ne sera pas livré avant la prochaine mise à jour régulière de l'éditeur allemand.

Cette nouvelle faille qui touche l'offre SAP intervient après la récente livraison de Java 7 par Oracle. **Nouvelle version qui s'est rapidement révélée boguée à son tour**. Au point de créer la polémique au sein de la communauté Apache sur le projet Lucene. Oracle a, lui aussi, promis de corriger rapidement le problème.

Crédit photo : © nali – Fotolia.com