Après SAP, les ERP d'Oracle étalent leurs multiples failles de sécurité

Après les multiples failles touchant les environnements SAP, au tour de l'ERP eBusiness Suite d'Oracle de subir les assauts des chercheurs en sécurité. Lors de la récente conférence BlackHat, David Lichtfield, un chercheur en sécurité qui a l'habitude de mettre à rude épreuve les environnements Oracle, s'est penché sur l'ERP de l'éditeur de Redwood Shores. Première remarque du chercheur : comme pour SAP, il s'agit là d'environnements gigantesques, offrant une surface d'attaque « *gargantuesque* », note Lichtfield dans sa présentation. Qui ajoute : « *Et nous savons tous ce que signifie une importante surface d'attaques* ». Comprendre des possibilités de compromission décuplées.

Au passage, le chercheur s'amuse des fanfaronnades de l'éditeur, qui, dans son guide de configuration de sécurité de la version 11i de la eBusiness Suite, affirme : « *Parmi les injections SQL potentielles qui nous ont été décrites, nous n'avons pas encore trouvé un cas confirmé (d'attaque de ce type, NDLR).* » Or, c'est précisément sur un ERP de cette génération – il est vrai un peu vieillissante – que le chercheur a fait la moisson de failles la plus étoffée. En novembre dernier, en une semaine, David Lichtfield a déniché et communiqué à Oracle 50 failles, dont 21 par injection SQL et 26 par cross-site scripting (ou XSS). Il lui a « suffi » de passer au crible 15 000 pages JavaServer (JSP), la passerelle PL/SQL (retirée de la version 12), le serveur de base de données ou encore le Concurrent Processing Server (le module assurant le traitement de données en tâche de fond). Un environnement complexe donc, qui renferme « *de nombreux fruits bien juteux qu'un assaillant s'empressera de scruter et tentera de compromettre* », dit Lichtfield. Et ce dernier de s'étonner que le code de cette version 11, qui remonte à 2001, n'ait pas été davantage amélioré au cours de toutes ces années. « *Oracle affirme avoir mis en place un processus solide pour éviter cela (la présence de failles par trop évidentes, NDLR) ; cette affirmation mérite d'être questionnée* », note-t-il.

Bugs signalés mais non corrigés

Après environ 80 heures passées sur une version 12.2, la liste de vulnérabilités publiée par David Lichtfield est un peu moins impressionnante, mais renferme tout de même deux failles liées à la dé-sérialisation Java, 8 injections SQL, une exposition de cookie, une attaque par déni de service ou encore un grand nombre de vulnérabilités par cross-site scripting notamment. Et certains de ces bugs ne sont pas encore corrigés par l'éditeur, regrette le chercheur qui lui a pourtant fait part de ses découvertes en avant-première. « *Les failles par injection SQL sont les plus critiques car elles permettent une compromission totale du serveur de base de données et de toutes ses données sans login ni mot de passe* », précise le chercheur.

Pour diminuer la fragilité des environnements eBusiness Suite, le chercheur suggère avant tout de réduire la surface d'attaque, en scrutant les logs d'accès aux composants. Et de citer un exemple récent où il a ainsi pu passer de 15 000 JSP à moins de 200 et de 80 Servlets à 2.

A lire aussi :

Sécurité : SAP, un nid de failles trop longtemps négligé

CITL : Un hacker évalue gratuitement la sécurité des logiciels

Crédit photo © Pavel Ignatov – shutterstock