Une faille dans un composant expose des milliers d’applications Java | Le Net Expert Informatique

Une faille dans un composant expose des milliers d’applications Java

Découverte il y a 9 mois, une vulnérabilité non corrigée dans le composant Apache Commons Collections expose les serveurs d'applications Java à un sérieux risque d'exécution de code à distance.

La dernière faille critique Java en date a été découverte dans la bibliothèque Apache Commons qui regroupe un ensemble de composants Java dont la maintenance est assurée par l'Apache Software Foundation. La bibliothèque est utilisée par défaut dans plusieurs serveurs d'applications Java et dans des produits comme Oracle WebLogic, IBM WebSphere, JBoss, Jenkins et OpenNMS.

La vulnérabilité, précisément localisée dans le composant Collections d'Apache Commons, résulte directement de la désérialisation des objets Java. Dans les langages de programmation, la sérialisation désigne le processus de conversion des données en format binaire. Cette conversion permet le stockage des données dans un fichier ou dans la mémoire, ou leur envoi sur le réseau. La désérialisation est le processus inverse.

La vulnérabilité, signalée par les chercheurs Chris Frohoff et Gabriel Lawrence en janvier 2015 pendant une conférence sur la sécurité, n'a pas suscité beaucoup d'attention. Sans doute que la plupart des gens estiment que la responsabilité de la prévention des attaques exploitant le processus de désérialisation incombe aux développeurs d'applications Java et non aux créateurs de la bibliothèque.

« Je ne pense pas qu'il faut incriminer la bibliothèque, même si elle peut certainement être améliorée », a déclaré par courriel Carsten Eiram, responsable de la recherche dans l'entreprise de sécurité Risk Based Security.

« En définitive, une entrée non fiable ne devrait jamais être désérialisée aveuglément. Les développeurs devraient comprendre comment fonctionne une bibliothèque et valider chaque entrée au lieu de lui faire confiance ou espérer qu'elle effectue à leur place ce travail de sécurisation ».

Un correctif bientôt disponible

Vendredi dernier, la faille est revenue dans l'actualité : les chercheurs de l'entreprise de sécurité FoxGLove ont livré des exploits proof-of-concept pour WebLogic, WebSphere, JBoss, Jenkins et OpenNMS basés sur la vulnérabilité. Mardi, Oracle a publié un avis de sécurité comportant des instructions d'atténuation temporaires pour WebLogic Server en attendant le correctif permanent que l'éditeur est en train de mettre au point. Les développeurs d'Apache Commons Collections ont également commencé à travailler sur un correctif.

Apache Commons Collections contient une classe InvokerTransformer. La faille utilise la sérialisation Java et une méthode d'appel dynamique dite de réflexion sur la classe InvokerTransformer pour exécuter du code distant. Un attaquant pourrait fabriquer un objet sérialisé avec un contenu malveillant pour qu'il soit exécuté au moment de sa désérialisation par une application Java avec l'aide de la bibliothèque Apache Commons. « Prises séparément, la classe InvokerTransformer et la sérialisation ne sont pas en cause, mais dès qu'elles sont combinées, la question de sécurité apparaît », a déclaré Joshua Corman, CTO de Sonatype, une entreprise d'automatisation de la chaîne d'approvisionnement des logiciels qui aide les développeurs à suivre et à gérer les composants qu'ils utilisent dans leurs applications.

D'autres composants Apache Commons vulnérables

Joshua Corman et Bruce Mayhew, un autre chercheur en sécurité de Sonatype, pensent que le problème ne concerne pas uniquement le composant Collections d'Apache Commons. Selon eux, d'autres composants Java pourraient poser un problème identique. « Je peux vous assurer qu'aujourd'hui, un tas de gens passent les composants les plus courants au peigne fin pour identifier d'autres classes sérialisables qui pourraient permettre l'exécution de commandes à distance », a déclaré Bruce Mayhew. « Et parmi eux, il y a des gens bien intentionnés, mais probablement aussi des gens mal intentionnés ». Si l'on en croit les discussions en cours sur la recherche de bogues, InvokerTransformer n'est sans doute pas la seule classe vulnérable de l'environnement Apache Commons Collections. Trois autres classes pourraient présenter le même problème. Les chercheurs de FoxGLove Security se sont intéressés de près à des projets de logiciels publics utilisables en « commons-collection » hébergés sur GitHub et ils ont identifié 1300 sources possibles. Et il faut aussi prendre en compte les milliers d'applications Java qui utilisent la bibliothèque dans les environnements d'entreprise.

Même s'il y a une forte probabilité que le problème dépasse le composant Collections, les développeurs devraient essayer de retirer les commons-collections du classpath ou de supprimer la classe InvokerTransformer du fichier jar concerné tant qu'il n'y a pas de correctif disponible pour la vulnérabilité. Mais tous ces changements doivent être appliqués avec précaution, car ils peuvent rendre les applications inopérantes.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-faille-dans-un-composant-expose-des-milliers-d-applications-java-62956.html

Par Lucian Constantin, IDG NS (adaptation Jean Elyan)