Une faille Apache Struts menace 65% des entreprises du Fortune 100

Apache Struts, le framework MVC (Model–view–controller) de développement d'applications web Java EE, est victime d'une sévère faille de sécurité. Celle-ci réside plus particulièrement dans le plugin de communication REST, très utilisé dans les déploiements de Struts en entreprise.

« Toutes les versions de Struts depuis 2008 sont affectées, indique le site communautaire d'analyse de code Open Source Lgtm.com. *Toutes les applications Web utilisant le populaire plugin REST du framework sont vulnérables. »* Et de conseiller *« vivement »* aux utilisateurs d'adopter la dernière version de l'outil pour limiter les risques d'attaque, à savoir la 2.5.13.

Exécuter du code arbitraire distant

Référencée CVE-2017-9805, la vulnérabilité permet à un attaquant distant d'exécuter un code arbitraire sur n'importe quel serveur exécutant une application construite sous Struts et utilisant REST. La faille réside dans la façon dont Struts « désérialise » les données non fiables. Pour mitiger les risques d'attaque, Man Yue Mo, le chercheur à l'origine de la découverte le 17 juillet dernier, n'exposera pas son modèle d'exploitation de la faille dans sa contribution mais propose une méthode (une requête QL) pour identifier les situations dans lesquelles des données non saines sont désérialisées dans un objet Java.

Pour l'heure, aucune attaque exploitant la faille n'est à déplorer, assure Lgtm. Mais, maintenant que le bug de sécurité a été dévoilé,*« il est probable qu'il va bientôt y en avoir »*, craint l'organisation. Une probabilité qui menace au moins 65% des entreprises du Fortune 100, estime Fintan Ryan, analyste pour le cabinet RedMonk. *« Des organisations comme Lockheed Martin, l'IRS, Citigroup, Vodafone, Virgin Atlantic, Reader's Digest, Office Depot et Showtime sont connues pour avoir développé des applications utilisant le framework*, souligne Lgtm. *Ceci illustre l'ampleur du risque. »*

Lire également
90% des entreprises attaquées par des failles de plus de 3 ans
Une faille zero day sur les serveurs Apache massivement exploitée
La Fondation Apache adoube les projets Open Source Beam et Eagle

Crédit Photo : Vchal-Shutterstock