# ParseDroid menace les développeurs d'applications Android

L'environnement Android se retrouve de nouveau exposé à des risques d'attaques majeures. Cette fois, le danger vient des outils de développement d'applications de l'OS mobile de Google qui exploite le langage Java.

*« Les vulnérabilités en question sont les outils de développement, à la fois téléchargeables et dans le Cloud, que l'écosystème d'applications Android, la plus grande communauté d'applications au monde, utilise*, pointent les chercheurs en sécurité de Check Point. *Cela inclut les outils que tous les programmeurs Java/Android utilisent pour construire leurs applications métier et que les analystes en sécurité et les d'ingénierie inversée utilisent pour leurs travaux. »*

## Tous les outils de développements Android affectés

La firme de sécurité a trouvé des vulnérabilités dans la plupart des outils de développement, dont Android Studio de Google, IntelliJ IDEA de JetBrains ou encore le framework Open Source Eclipse de la fondation éponyme. APKTool, le service Cuckoo-Droid et d'autres sont également concernés. Ces vulnérabilités baptisées ParseDroid affectent la bibliothèque d'analyse XML des outils de développement.

Et Check Point de détailler, dans son billet de blog, comment les chercheurs ont réussi à exploiter ses failles pour accéder à des fichiers sur des machines affectées, voire exécuter du code malveillant.

## Tous les OS concernés

*« La vulnérabilité expose l'ensemble des fichiers système de l'OS des utilisateurs d'APKTool, et par conséquent, les attaquants pourraient potentiellement récupérer n'importe quel fichier sur le PC de la victime en utilisant un fichier malveillant 'AndroidManifest. Xml' qui exploite une vulnérabilité XXE (XML External Entity, NDLR), qui pourrait ensuite être envoyé à un serveur attaquant distant*, écrit l'équipe de recherche. *Et ce scénario d'attaque n'est qu'une des nombreuses techniques d'attaque XXE possibles qui pourraient mener à des conséquences néfastes. »*

Une vulnérabilité qui, par l'universalité d'APKTool, concerne tous les principaux OS du marché, Windows, macOS ou Linux. *« Il est également possible d'attaquer tout système sur lequel il fonctionne sans restriction ni limitation »*, poursuivent les chercheurs en sécurité.

Check Point a informé les principaux éditeurs et développeurs concernés de sa découverte en mai 2017. Lesquels ont, pour la plupart, fourni un correctif. Les utilisateurs de ces outils de développement n'ont plus qu'à s'assurer l'avoir appliqué.

**Lire également**

**Android: une faille redoutable peut enclencher une attaque par recouvrement**
**WhatsApp: une fausse version téléchargée un million de fois sur Google Play**
**SonicSpy contamine plusieurs milliers d'apps Android**

**Photo credit: edowoo via VisualHunt / CC BY-SA**