Les serveurs back-end des apps mobiles ouverts à tous les vents

La faiblesse des systèmes de sécurité des bases de données mettrait en danger les données des applications mobiles des utilisateurs en entreprise. Selon une étude de Appthority, de larges pan de données sont exposés depuis et vers les plates-formes de back-end qui hébergent les outils de bases de données, relationnelles ou non, dont Elasticsearch, Redis, MongoDB, MySQL, CouchDB ou Couchbase… La faute n'en revient pas directement aux gestionnaires de bases de données mais à l'absence d'implémentations de systèmes d'authentification et de firewall entre les applications et les serveurs de back-end.

Conséquence, les informations stockées sur les serveurs peuvent facilement être extraites ou prises en otage par des pirates. Il suffit d'un peu d'ingénierie inversée et de scanning, selon le fournisseur de solutions dédiées à la sécurité mobile. C'est d'autant plus problématique que les entreprises n'ont que peu de contrôle sur la protection de leurs données dans la mesure où la faille réside sur les serveurs des fournisseurs. *« Seules les améliorations de la configuration de la plate-forme de back-end et éventuellement les modifications de code dans l'application affectée élimineront la vulnérabilité*, assure Appthority dans son rapport cité par *Darkreading*. *Si la vulnérabilité est exclusivement sur le back-end, même la mise à jour de l'application ne résoudra pas le problème. »*

Plus de 1000 applications concernées

Selon les experts en sécurité mobile, plus de 1000 applications exposent ainsi les données des organisations qui les utilisent à travers des bases de données. Appthority s'est concentré sur 39 d'entre elles, proposées par des éditeurs respectables et attentifs aux pratiques de sécurité, pour constater que 280 millions d'enregistrements étaient exposés. Face à l'immense volume de contenus ainsi disponibles (43 To), les chercheurs se sont limités au cas d'Elasticsearch, l'outil d'indexation.

« Elasticsearch n'a pas intégré la sécurité et le contrôle d'accès et s'appuie sur la mise en œuvre externe de ces fonctionnalités de sécurité avec un plugin d'authentification ou une API pour l'accès, par exemple, commente le rapport. *Si le serveur Elasticsearch est accessible publiquement sur Internet sans ces fonctionnalités de sécurité, les données stockées seront disponibles pour toute personne qui sait où regarder. »*

Les entreprises exposées

Et les cyber-criminels savent où regarder. En début d'année, les données de plusieurs instances d'Elasticsearch ont fait l'objet de rançonnage. Le système Open Source d'indexation n'était d'ailleurs pas le premier. Des bases de données MongoDB en avaient également fait les frais peu de temps avant. En l'absence de système d'authentification, 21 000 instance d'Elasticsearch seraient aujourd'hui exposées, avance Appthority.

« Chaque nouvelle application mobile qui utilise une plate-forme de back-end pour le stockage ou l'analyse de

données est une source potentielle de risque, avertit le rapport. *Les entreprises qui s'appuient sur les développeurs de logiciels pour coder et configurer correctement les connexions du back-end sont exposées.* »
Celles qui n'auraient pas déjà été victimes d'un piratage sont maintenant prévenues.

Lire également
Bases MongoDB rançonnées : l'infection se propage à vitesse grand V
Un hacker tombe par hasard sur des bases MongoDB non protégées
Apple n'a pas été piraté, mais 250 millions de ses utilisateurs sont bien menacés

crédit photo © Kirill Wright – shutterstock