Sécurité : plus de 300 vulnérabilités à combler chez Oracle

C'est à un update maousse auquel vont devoir s'attaquer les administrateurs Oracle : l'éditeur de Redwood Shores vient en effet de livrer le plus gros lot de correctifs de sécurité de son histoire. Son Critical Patch Update de juillet comble en effet pas moins de **308 vulnérabilités, dont 165 sont exploitables à distance**. Plus de 90 produits différents sont concernés. C'est plus que le précédent Update d'avril dernier, qui renfermait déjà des correctifs pour 300 failles.

Au total, depuis le début de l'année 2017, Oracle a comblé pas moins de 878 vulnérabilités, au travers de trois Critical Patch Update. Soit un véritable déluge de correctifs pour les administrateurs. Comme l'ont montré les crises WannaCry et NotPetya – dont la diffusion reposait sur des failles connues de Windows -, les équipes IT peinent à patcher rapidement les systèmes de leurs organisations. Le temps nécessaire à la qualification des correctifs sur les systèmes d'une entreprise suffit souvent aux assaillants pour lancer des exploits basés sur les failles révélées par les éditeurs.

Récupérer les données de l'ERP sans authentification

Au sein du dernier Critical Patch Update d'Oracle, L'ERP E-Business Suite apparaît comme le plus exposé. Le progiciel concentre pas moins de 120 vulnérabilités, dont 118 sont exploitables à distance. L'une de ces failles (CVE-2017-10244), dévoilée à l'éditeur par la société Onapsis en avril, apparaît comme particulièrement dangereuse : elle permet à un assaillant de **télécharger des données de l'ERP sans authentification**. Un boulevard pour rapatrier des données confidentielles d'une entreprise sur E-Business Suite, d'autant qu'il est assez facile d'identifier des cibles potentielles via Google ou Shodan. A patcher en urgence donc, même si l'exploitation de cette vulnérabilité nécessite de récupérer des paramètres spécifiques à l'implémentation afin de forger une requête HTTP malveillantes. Mais, dans bien des cas, les éléments exposés sur Internet suffisent pour y parvenir, assure Onapsis.

Oracle Fusion Middleware et Java SE se contentent de 18 et 17 vulnérabilités respectivement, mais 16 défauts sont exploitables à distance dans chacun de ces produits. 7 bugs de Fusion Middleware ont un score CVSS (système d'évaluation standardisé de la criticité des vulnérabilités) d'au moins 8,6, avec trois défauts exploitables à distance dans Oracle Outside In Technology, Tuxedo et WebLogic Server évalués à 9,8.

Trois failles pour Database Server

Trois vulnérabilités Java SE, Java SE Embedded et JRockit reçoivent un score CVSS d'au moins 9,0 ; toutes sont exploitables à distance et affectent plusieurs versions du logiciel concerné.

Oracle corrige également 37 vulnérabilités dans la suite Oracle Financial Services Applications, dont 14 exploitables à distance. Enfin, signalons cinq correctifs pour la base de données Oracle Database

Server, dont trois concernent des failles exploitables à distance dans les composants Oracle Secure Backup et Oracle Big Data Graph du serveur.

A lire aussi :

Oracle colmate près de 300 failles pour son Critical Patch Update

Un sysadmin plastique la base Oracle de son ex-employeur

Crédit photo : Katherine Welles / Shutterstock.com