Oracle relance le débat sur le ‘full-disclosure ‘

La société Red Database Security, spécialisée dans la sécurité des bases de données Oracle, vient en effet de publier des informations relatives à 6 failles, dont 3 sont considérées à haut risque. Parmi la liste des alertes publiées sur le site de la société, il est surprenant d’ailleurs de constater que certaines failles classiques (CSS) ont plus de 720 jours.

« Le comportement d’Oracle, en ne fixant pas certains bugs critiques connus depuis longtemps (plus de 650 jours) n’est pas acceptable pour ses clients », indique Alexander Kornburst, CEO est chercheur principal de Red Database Security. Cette histoire, qui a le mérite de relancer le débat sur le ‘full-disclosure’ et les modalités de publication des vulnérabilités, ravive les tensions qui existent parfois entre les chercheurs indépendants en sécurité et les éditeurs de logiciel. Certains d’entre eux, comme Sybase ou Microsoft par exemple, ont tenté dernièrement de gagner la sympathie des chercheurs. Ainsi, la firme de Redmond a fait une présentation remarquée au dernier CanSec West où elle expliquait sa méthodologie de gestion des failles de sécurité. Oracle Unbreakable ? En ce qui concerne Oracle, non seulement la société communique maladroitement avec les chercheurs, mais elle ne propose aucun correctif pour les failles découvertes. *« Nous pensons que la manière la plus efficace de protéger nos clients consiste à éviter de divulguer ou de publier le détail des failles avant qu’un patch ait été développé »*, a déclaré récemment la compagnie. Red Database a pourtant alerté Oracle entre juillet et septembre 2003 à propos de plusieurs failles sérieuses. Elle a ensuite lancé un ultimatum à l’éditeur, lui laissant jusqu’à la date de sortie du patch trimestriel du mois de juillet avant de publier les failles. Dans la mesure où aucune des failles n’a été corrigée dans la dernière mise à jour, Red Database a édité 6 bulletins d’alertes. *« J’ai décidé de publier ces vulnérabilités car il est possible de réduire le risque en utilisant les solutions de contournement mentionnées dans les bulletins »*, poursuit Alexander Kornburst. Alors que Oracle semble adopter ici une stratégie de ‘sécurité par l’obscurité’, rappelons simplement que le délai moyen entre la publication d’une faille et son exploitation par un ver est actuellement de l’ordre de 10 jours. Heureusement que les cybercriminels ciblent davantage la firme de Redmond que celle de Redwood? **Thierry Evangelista** pour **Vulnerabilite.com**