Oracle: une faiblesse dans la protection des mots de passe

La faille découverte permettrait de recouvrir les mots en clair à partir de leur correspondance chiffrée. Les mots de passes les plus compliqués ne prendraient que quelques minutes à être cassés.

Selon Joshua Wright du SANS Institute et Carlos Sid du Royal Holloway College (Université de Londres) la technique utilisée pour chiffrer et stocker les mots de passes n'offre pas un niveau de sécurité suffisant : *« En exploitant ces faiblesses, un intrus ayant accès à des ressources limitées pourrait initier une attaque qui permettrait de révéler le mot de passe en clair d'un utilisateur connu »*. Lors de sa présentation Wright a exposé l'algorithme de chiffrement incriminé et a effectué une démonstration en temps réel de l'outil qu'il a développé pour réaliser l'attaque cryptographique. Une des faiblesses majeures réside dans le fait que ces mots de passes sont convertis en caractères majuscules avant d'êtres chiffrés, ce qui réduit considérablement l'alphabet utilise. Les deux chercheurs ont informé Oracle en Juillet dernier. Malheureusement leurs requêtes sont jusqu'alors restées sans réponse. Un document proposé par Wright et Sid qui expose plus en détail la vulnérabilité est disponible sur le site Web du SANS Institute. **Norman Girard** pour **Vulnerabilite.com**.