

# Oracle demande à ses clients de ne pas appliquer certains correctifs de sécurité

Dans le domaine de la sécurité, le temps ne joue pas en faveur des cibles potentielles. Mais sa pression explique aussi sans doute l'erreur commise dans l'un des correctifs de sécurité édité le 18 janvier : à cause d'une simple faute de frappe, les entreprises exploitant une base de données Oracle en version 8.1.7.4 sur Solaris doivent réinstaller une version antérieure du patch. Surprise ! Cette version n'est pas datée du 18 janvier, mais du 15 février. Il s'agissait donc d'un patch déjà patché? Le correctif Oracle concerné est référencé « Patch 4751906 ». Par ailleurs, on notera qu'à ce jour, la faille DayZero révélée le 25 janvier par David Litchfield lors des derniers BlackHat n'est toujours pas corrigée. De son côté, Microsoft a invité ses clients à réinstaller une nouvelle version de son correctif MS06-007 dont l'installation à partir d'Automatic Update, Windows Update ou par l'outil WSUS ne s'effectue pas correctement en cas d'utilisation combinée avec ITMU (outil d'inventaire). En face de ces incidents, quelle stratégie adopter ? Appliquer rapidement les correctifs proposés par les différents éditeurs, en espérant qu'ils ne créent pas d'incident de production ni de régressions fonctionnelles (démarche dite « Patch and Pray ») ou attendre la stabilisation des correctifs ? en restant exposés aux exploits ?

**Bruno Rasle pour [Vulnerabilite.com](http://Vulnerabilite.com)**