Les sites de Sun et MySQL piratés

Mauvais coup de pub pour Oracle. Des individus malveillants sont parvenus à récupérer des données confidentielles sur les serveurs de l'entreprise par le biais d'une injection SQL. Cet acte serait l'œuvre de deux pirates roumains 'TinKode' et 'Ne0h'.

Le premier a indiqué sur son blog que deux sous-domaines du site de Sun Microsystems (désormais propriété d'Oracle) ont été compromis. Ainsi que le site MySQL.com et un domaine rattaché à l'éditeur de sécurité Eset d'origine roumaine.

Selon a *eWeekEurope*, le hacker TinKode a pu obtenir les noms de tables, de colonnes et d'adresses électroniques enregistrées dans l'une des tables de la base de données. A ce stade, il n'est pas établi que le pirate ait pu avoir accès aux mots de passe du site Sun.com ou si cette information est passée sous silence pour une raison quelconque.

Les exploitations de failles par injection SQL sont certes courantes. Mais les équipes de développement web d'Oracle-Sun risquent de recevoir une pluie de critiques. *« Le problème ne vient pas du logiciel de base de données open source (MySQL) mais de la façon dont le site Web a été codé »*, explique Chester Wisniewski, un expert de Sophos, sur le blog Naked Security.

Chester Wisniewski rappelle dans sa contribution la nécessité de réaliser des audits de son code à intervalles réguliers, et d'utiliser des mots de passe complexes, au risque de se retrouver dans des situations inconfortables vis-à-vis de ses clients/utilisateurs ou même de ses concurrents. Pour Oracle, le travail de sécurisation vient juste de commencer.

En effet, des experts en sécurité présents sur le site XSSed (spécialisé dans les failles XSS) pointent du doigt les sites MySQL.com et Sun.com qui comporteraient *« un certain nombre »* de vulnérabilités cross-site-scripting, à ce jour non-corrigées. Elles auraient d'ailleurs pu être utilisées dans le cas de la récente attaque mais cela n'a pas été établi. Oracle ne pouvant régler immédiatement le problème pour Sun.com, le nom de domaine a été redirigé vers une page interne du site de l'éditeur.