



AVIS D'EXPERT

OLIVIER DEMBOUR

CONSULTANT SÉCURITÉ CHEZ HERVÉ SCHAUER CONSULTANTS

« Avantage à l'Open Source pour la publication des correctifs »

Les vulnérabilités exploitables connues des éditeurs et non encore corrigées constituent un sujet sensible pour les grandes entreprises. Sur ce point, dans le domaine particulier de la sécurité, il existe une différence notable de traitement entre les produits commerciaux et les produits libres.

Pour les logiciels à code ouvert, lorsqu'une personne découvre une vulnérabilité sur un logiciel, elle est généralement capable de comprendre d'où vient le problème et comment le corriger. Elle est donc capable de soumettre une proposition de correction. La communauté pourra ensuite l'auditer et, au besoin, l'améliorer. Le cycle de gestion des correctifs se trouve être relativement court. Quant à la fiabilité du code, il est obtenu grâce au partage du code avec

la communauté de développeurs travaillant sur le projet.

Dans le monde commercial, les éditeurs ont la responsabilité de la correction des failles. Et il n'est pas rare de constater des délais très longs. Ainsi Microsoft, société prenant pourtant particulièrement au sérieux les problématiques de sécurité, admet qu'un correctif met environ six mois avant d'être publié. Ce délai englobe les tests de compatibilité et de régression. Certains constructeurs comme Oracle, ont une politique très différente, obligeant les chercheurs à diffuser publiquement les détails des failles pour espérer un correctif. Seulement, l'éditeur a déjà mis 1 221 jours pour corriger une faille. Cette situation totalement inacceptable ne pourrait tout simplement pas être possible dans un produit libre. ■