McAfee étoffe sa gamme de produits anti-Heartbleed

La vulnérabilité Heartbleed a fait couler beaucoup d'encre. Et pour cause, puisqu'elle touche OpenSSL, et donc la plupart des sites web sécurisés présents sur la Toile (voir « Heartbleed : la faille qui met OpenSSL, et la NSA, sur la sellette »).

Il y a dix jours, McAfee mettait en ligne un outil gratuit permettant vérifier si un site web était concerné par cette vulnérabilité (voir l'article « Heartbleed : McAfee met en ligne un outil de test dédié aux internautes »).

Deux autres initiatives

L'éditeur américain complète aujourd'hui cette offre avec une application permettant de détecter si un smartphone ou une tablette Android est concerné par cette vulnérabilité (car Android utilise lui aussi OpenSSL). Cet outil est accessible gratuitement sur Google Play.

Dans le même temps, la firme explique comment les utilisateurs de sa Web Gateway peuvent empêcher l'accès aux sites touchés par Heartbleed. Une procédure détaillée sur cette page web.

Dans l'ensemble, le correctif d'OpenSSL a été appliqué relativement rapidement. Plusieurs initiatives ont également été lancées afin d'éviter qu'un tel problème se reproduise dans le futur. La première sous l'égide de la Fondation Linux, qui souhaite améliorer la qualité des logiciels open source, et la seconde par l'équipe d'OpenBSD, qui lance LibreSSL, un dérivé ultra sécurisé d'OpenSSL.

Voir aussi
Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales