Faille Shell Shock : la Free Software Foundation réagit promptement

Une faille critique vient d'être découverte dans l'interpréteur Bash. Elle permet de lancer du code distant sur un serveur, chose qui peut se montrer potentiellement très dangereuse, en particulier si vos processus serveur fonctionnent avec des droits étendus (voir l'article « Shellshock : une faille dans Bash à la hauteur de Heartbleed »).

Bash est un logiciel libre faisant partie du projet GNU. La **Free Software Foundation** se devait de réagir sans délai. Ce qu'elle a fait : *« les problèmes les plus graves ont déjà été corrigés, et une solution complète est en bonne voie. Les distributions GNU/Linux travaillent rapidement à la publication de mises à jour. Tous les utilisateurs de Bash doivent installer immédiatement les mises à jour et vérifier la liste des services réseau en cours d'exécution sur leurs systèmes. »*

Les opérations de mise à jour de Bash devraient être grandement facilitées par le fait que la plupart des OS Linux utilisent des gestionnaires de paquets prenant en compte cette problématique.

Red Hat à la manœuvre

« Le logiciel libre est une condition préalable pour une informatique sécurisée, poursuit la FSF. *Il garantit à chacun la possibilité d'examiner le code pour détecter des vulnérabilités, et les corriger. Cette liberté ne garantit pas un code sans bogue, pas plus que dans les logiciels propriétaires : des bogues peuvent survenir, quelle que soit la licence utilisée. Mais quand un bogue est découvert dans un logiciel libre, tout le monde à l'autorisation, les droits et le code source nécessaire pour exposer et résoudre le problème. »*

En l'occurrence, c'est ici Red Hat qui s'est rapproché des équipes de développement du projet Bash et leur a fourni un correctif. Des patches pour Bash 3.0, 3.1, 3.2, 4.0, 4.1, 4.2 et 4.3 sont accessibles directement sur le FTP du projet GNU.

Sur le même thème

Alerte aux failles de sécurité pour Adobe Reader et Adobe Acrobat
5 mois après : le bilan de la faille Heartbleed