Une brèche de sécurité « zero day » est ouverte dans le noyau Linux

Une faille de sécurité critique a récemment été découverte dans le noyau Linux (CVE-2012-0056). Cette dernière permet, par escalade de privilèges, d'obtenir les droits d'administration depuis un compte utilisateur ordinaire.

Le correctif permettant de combler cette vulnérabilité a été livré le 17 janvier, par **Linus Torvalds**, le créateur du noyau Linux. Il a été directement rendu public, chose qui ne pose en général pas de problème… sauf dans ce cas précis.

Les *hackers* se sont en effet montrés particulièrement efficaces. Ils ont réussi à mettre au point un *exploit* en un temps record (ce dernier est disponible depuis le 22 janvier). Mempodipper met toutes les versions du noyau Linux depuis la 2.6.39 à découvert.

Vite, vite, vite

Une course contre la montre s'est engagée chez les éditeurs de distribution Linux, afin d'appliquer le plus rapidement possible le correctif proposé le 17. Les offres signées Red Hat, Ubuntu et ArchLinux sont d'ores et déjà à l'abri de l'*exploit*. Espérons que les autres acteurs du marché se montreront aussi réactifs.

Les machines fonctionnant sous Android 4.0 sont également touchées (une version adaptée de mempodipper a même été créée : mempodroid). Voilà qui est bien plus épineux, l'OS mobile de Google étant mis à jour beaucoup moins régulièrement que les distributions Linux traditionnelles.