# Mauvaise passe pour l'antivirus ClamAV

Secunia a dévoilé deux failles critiques qui touchent le moteur de l'antivirus *open source* ClamAV (placé sous licence GPL).

Les exécutables Windows (au format PE et compressés avec Upack ou PESpin) peuvent provoquer un dépassement de tampon. **Un*exploit*a été publié concernant la première vulnérabilité** : il permet l'exécution de code distant sur la machine utilisant ClamAV. Notez que le traitement de certaines archives ARJ peut aussi mener au plantage de l'application.

Ces failles sont fort heureusement sans grande incidence dans la pratique. ClamAV est utilisé essentiellement sur les serveurs de courrier électronique, où il se charge d'intercepter les virus transitant dans les *emails*. En général, il est lancé avec des droits restreints, interdisant ainsi la prise de contrôle de la machine par un pirate en cas de plantage grave.

L'équipe de développement de ClamAV a par ailleurs coupé le moteur de vérification des exécutables PE au travers des mises à jour quotidiennes de l'antivirus, et ceci dès le 10 mars dernier (soit plus d'un mois avant l'annonce de Secunia). Une grande majorité des machines est donc restée à l'abri de ces failles.

Enfin, **la dernière mouture stable de ClamAV, estampillée 0.93, corrige tous ces problèmes**. Les administrateurs système sont priés de la télécharger et de l'installer sans tarder.