L’antivirus open-source ‘Clamav’ vulnérable

Neel Mehta et Alex Wheeler, tous deux employés par la société ISS, ne semblent pas avoir perdu la foi qui les animait lors de la conférence BlackHat Europe 2005 à Amsterdam. Les deux compères s’évertuaient à expliquer leurs méthodes de détection de vulnérabilités au sein de la plupart des antivirus du marché. Après McAfee, Symantec, Trend Micro, F-Secure, aujourd’hui c’est ClamAV, l’antivirus open-source, qui s’y colle.

En effet, les deux chercheurs viennent de mettre en avant trois vulnérabilités critiques affectant l’antivirus open-source. Les trois défauts de sécurité se situent au c?ur des fonctionnalités de traitement des formats de fichiers TNEF, CHM et FSG. En forçant l’antivirus à ‘scanner’ un email piégé, il serait possible d’exécuter du code arbitraire avec les doits associés au processus ClamAV. Les versions ClamAV 0.86.1 et inférieures sont vulnérables. Une mise à jour vers la version 0.86.2 s’impose pour rester hors de portée des pirates. **Vous utilisez peut-être ClamAV sans le savoir !** L’antivirus GPL ClamAV offre bien des avantages aux constructeurs d’appliance de sécurité. De nombreuses solutions commerciales intègrent ClamAV et beaucoup d’utilisateurs l’ignorent. Si vous utilisez, par exemple, des boîtiers de sécurité Watchguard Firebox, Barracuda, Adytone ou encore AutumnTECH, il est possible que vous soyez vulnérable. Rapprochez-vous donc rapidement de votre revendeur ou constructeur pour profiter de la mise à jour de ClamAV. **Aurélien Cabezon** pour **Vulnerabilite.com**