

Une faille critique dans Winamp

Cela faisait longtemps que le célèbre lecteur audio de NullSoft n'avait pas fait parler de lui. D'après ATmaCA et Secunia, la faille est jugée « *très dangereuse.* »

Cette dernière, exploite un « buffer overflow » ou dépassement de mémoire tampon en français. Un bug qui peut être exploité par un spécialiste de l'intrusion.

Un attaquant pourrait utiliser cette faille qui touche la façon dont le programme gère la liste des titres (playlist) . Un attaquant suffisamment « ingénieux » serait à même de créer une playlist contenant des noms de fichiers trop longs (1040 bytes) et y placer un code malveillant.

Nullsoft, l'éditeur du célèbre logiciel de lecture de fichiers musicaux vient de publier [une nouvelle version de Winamp](#) (la 5.13) qui a pour seul intérêt de combler cette faille.

Notons que la version 5.2 devrait logiquement être disponible à partir du 20 février.

Pour l'instant, cette vulnérabilité n'a été confirmée que dans les versions 5.094, 5.12 et 5.11, mais d'autres versions pourraient bien être la cible de cette faille qui fonctionne sous XP SP2.

Les versions précédentes n'ont pas encore été testées, mais la prudence est de mise.