Faille critique dans Winamp, lecteur mp3

Le très célèbre lecteur de mp3 Winamp de NullSoft/AOL est victime d'une faille qualifiée d'extrêmement critique. Découverte par Silent et relayée par le site de Secunia, la vulnérabilité permettrait à un pirate de lancer n'importe quel programme à l'insu de l'utilisateur.

La faille se situe dans le système de 'skins' (ces habillages qui modifient l'interface) utilisé par Winamp et téléchargeables un peu partout. Le problème serait dû à des restrictions insuffisantes sur les fichiers compressés des skins de Winamp (.wsz), et plus particulièrement à un manque de sécurité dans l'architecture XML employée. Ce qui permet d'exécuter un programme inséré dans la 'skin'. *« La faille peut être exploitée par un site web malveillant qui utiliserait une 'skin' Winamp conçue spécialement pour placer et exécuter des programmes arbitraires »*, explique Secunia, avant d'ajouter que *« la vulnérabilité peut être exploitée sans interaction avec l'utilisateur dans un environnement Internet Explorer »*. Selon ces spécialistes, la faille est déjà largement exploitée par les concepteurs de modules espions ou spywares' et répandue à travers les réseaux IRC pour introduire ces modules ou autres virus/vers sur certains ordinateurs. L'ensemble des versions 3.x et 5.x de Winamp sont concernées. Il n'y a pas encore de 'patch'. Secunia conseille d'utiliser un autre produit.