Une faille critique frappe Winamp

Avec près de cinq millions d'utilisateurs (selon download.com), Winamp fait partie des lecteurs multimedias plébiscités par les internautes. Mais le logiciel développé par Nullsoft, une filiale d'AOL, représente également une cible de choix pour les pirates. Et ce n'est pas la première fois qu'ils s'attaquent au logiciel. C'est une faille de type 'buffer overflow' qui frappe aujourd'hui Winamp. Le dépassement de mémoire tampon s¹effectue au niveau du champ 'File' dont la longueur n'est pas vérifiée. L'exploitation de la vulnérabilité, à travers la lecture d'un fichier '.pls' piégé (fichier playlist), offre au pirate la possibilité d'exécuter du code arbitraire sur la machine de sa victime.

Un exploit 'proof-of-concept' est d'ores et déjà en circulation sur la toile. Ce code permet de créer un fichier '.pls' piégé qui, une fois exécuté, va déclencher l'ouverture du programme calculatrice de Windows (calc.exe). Jusqu'ici rien de très dangereux sauf qu'il suffit de modifier la charge utile (payload) de ce code pour en faire une arme destructrice. **Un possible vecteur de malwares** Il y a fort à parier que des individus peu scrupuleux vont se ruer sur cette nouvelle faille « de masse » pour véhiculer au plus grand nombre des malwares en tout genre, tels que spywares, adwares et autres virus. Toutes les versions de Winamp, y compris la dernière version 5.12 sont vulnérables. En attendant un correctif, évitez les fichier playlist ! Ce mardi, Nullsoft l'aditeur de Winamp, a mis en ligne la version 5.13 de Winamp qui corrige la vulnérabilité.