Failles critiques dans RealPlayer

Deux nouvelles failles touchent, encore une fois, les produits de RealNetworks. Découvertes par iDefense et NGS Software, elles sont qualifiées de hautement critiques par Secunia. Elles permettent de prendre le contrôle d'un système vulnérable à distance.

La première vulnérabilité résulte d'une erreur de type « buffer overflow » présente dans la gestion de certains fichiers « .wav ». Elle pourrait être exploitée afin d'exécuter des commandes arbitraires avec les privilèges de l'utilisateur connecté. La seconde faille résulte d'un problème « stack overflow » présent dans la gestion de certains fichiers « .smil », ce qui pourrait être exploité automatiquement via une page web malicieuse, afin d'exécuter des commandes arbitraires distantes. Des mises à jour sont disponibles à cette adresse: http://service.real.com/help/faq/security/050224_player/FR/ Versions impactées sous Windows : RealPlayer 10.5 (6.0.12.1056 et inférieures) RealPlayer 10 RealOne Player V2 RealOne Player V1 RealPlayer 8 RealPlayer Entreprise sous Mac : RealPlayer 10 (10.0.0.325 et inférieures) RealOne Player sous Linux : RealPlayer 10 Helix Player