Quatre failles critiques dans les produits Real

Des failles tous les mois. Depuis mars, les lecteurs RealPlayer et RealOne subissent des failles critiques. Certes corrigées, mais nombreuses. Cette fois, ce ne sont pas moins de quatre failles critiques qui ont été découvertes par NGSSoftware, iDEFENSE Labs, et eEye Digital Security. Ces vulnérabilités peuvent permettre une attaque distante.

Selon le site de veille FrSIRT, le premier problème résulte d'une erreur dansz le traitement des fichiers MP3, ce qui pourrait être exploité par des attaquants distants afin d'exécuter des contrôleurs ActiveX ou écraser des fichiers arbitraires présents au sein d'un système vulnérable. La seconde faille est due à une erreur de type heap overflow présente dans le gestionnaire RealText qui ne gère pas correctement certains fichiers RealMedia spécialement conçus, ce qui pourrait être exploité via un site web malicieux afin d'exécuter des commandes arbitraires avec les privilèges de l'utilisateur connecté. La troisième vulnérabilité résulte d'une erreur de type buffer overflow présente dans le fichier « vidplin.dll » qui ne traite pas correctement certains fichiers AVI spécialement conçus. FrSIRT explique que la faille pourrait être exploitée via un site web malicieux afin d'exécuter des commandes arbitraires distantes avec les privilèges de l'utilisateur connecté. Le dernier problème résulte d'une erreur inconnue qui, combinée à certaines versions d'Internet Explorer, pourrait permettre la création et l'exécution de fichiers malicieux au sein d'un système vulnérable. On ne saurait trop vous conseiller d'appliquer immédiatement les correctifs accessibles via l'option d emise à jour des logiciels concernés: RealPlayer 10, 10.5 (6.0.12.1040 à 6.0.12.1069) RealOne Player v1, v2 RealPlayer 8 RealPlayer Enterprise 1.1, 1.2, 1.5, 1.6, 1.7 Rhapsody 3 (build 0.815 à build 0.1006) Mac RealPlayer 10 (10.0.0.305 à 10.0.0.331) Mac RealOne Player Linux RealPlayer 10 (10.0.0 à 10.0.4) Helix Player (10.0.0 à 10.0.4)