Alerte : une vulnérabilité « zero-day » touche RealPlayer

Des hackers exploitent une vulnérabilité ‘zero-day’ qui touche RealPlayer, dans le but d’infecter les machines Windows qui utilisent le lecteur avec Internet Explorer.

L’éditeur de sécurité Symantec a publié une alerte de la catégorie « menace élevée », notée 10, ce qui correspond au niveau maximum de dangerosité.

Selon le réseau de surveillance du spécialiste de la sécurité informatique, le problème est provoqué par une faille dans un contrôle ActiveX publié par RealNetworks pour son lecteur multimédia : RealPlayer.

Ce bogue combiné à l’utilisation du navigateur de Redmond (ndlr : qui utilise ActiveX pour certaines fonctions avancées) représente un « danger important » estime Symantec qui explique dans une note publiée sur un blog : *« que cette faille peut être utilisée par des hackers pour envoyer du code malveillant sur un poste Windows. »*

Il semble d’ailleurs que des attaques soient déjà en route. Mais pour l’instant Symantec n’est pas en mesure de donner plus de détails. Par contre, dans son alerte, le groupe donne deux adresses IP qui semblent héberger ladite vulnérabilité ‘zero-day’.

Pour l’instant, RelaNetworks n’a pas publié de correctifs, et les dernières versions du lecteur, la 10.5 et la bêta 11 sont touchées.

Selon un blogueur, la NASA aurait diffusé une note interne interdisant à ses employés d’utiliser Internet Explorer.

Quoi qu’il en soit, l’éditeur recommande de désactiver le contrôle ActiveX impliqué en décochant le paramètre par défaut « Kill bit ». Il faut pour cela modifier une clé du registre, ce qui n’est malheureusement pas à la portée de tous les utilisateurs.