

# Microsoft corrige sa faille 0 Day sur les raccourcis

Microsoft doit livrer, dans la journée de ce lundi 2 août, un **correctif exceptionnel** visant à combler la faille du composant Windows Shell dévoilée le 16 juillet dernier. D'habitude, Microsoft livre ses correctifs de sécurité tous les deuxième mardi du mois. Sauf en cas d'urgence. La publication imminente d'un correctif montre donc la gravité de la situation.

Cette vulnérabilité (détaillée [ici](#)), qui affecte toutes les versions de Windows depuis XP SP3, permet notamment la prise de contrôle distante des machines affectées. Elle est due à une **mauvaise analyse par Windows des raccourcis** (fichiers .LNK et .PIF). Une personne mal intentionnée peut donc, à l'aide d'une icône de raccourci spécialement conçue, infecter un système soit localement (via une clé USB par exemple), soit à distance depuis le partage réseau et WebDAV. « *Un exploit peut également être inclus dans les types de documents spécifiques qui prennent en charge les raccourcis intégrés* », souligne encore l'éditeur.

Plusieurs malwares actifs permettent d'exploiter la «faille LNK». Citons notamment les agents (et leurs variantes) Stuxnet, Vobfus ou Chymine. **Holly Stewart**, du Microsoft Malware Protection Center, évoque également l'apparition d'un petit nouveau: **Sality**. Fortement Ce dernier a la fâcheuse tendance à infecter les fichiers du système, à se dupliquer sur les médias amovibles (clé USB...), à désactiver la sécurité, et à télécharger d'autres malwares.

Le danger d'infection est donc bien réel, notamment au Brésil, aux Etats-Unis, en Asie (Inde, Indonésie) et Moyen Orient (Iran) où il s'est principalement développé selon Microsoft. En résumé, il sera conseillé d'effectuer la mise à jour de sécurité dans les plus brefs délais.