

Une faille critique détectée dans Windows et Office !

Ce mardi, **Microsoft** a publié en urgence un correctif permettant de bloquer l'exploitation d'une faille zero-day découverte dans le composant traitant les images au format TIFF.

De nombreux produits sont concernés par cette vulnérabilité : les suites bureautiques Office 2003, Office 2007 et Office 2010, mais aussi Windows Vista, Windows Server 2008, Lync 2010 et Lync 2013.

Le « Fix it » fourni par Microsoft permet de bloquer les effets de cette faille. Il ne saurait toutefois remplacer un correctif, qui devrait être fourni ultérieurement. Vous trouverez le « Fix it » de Microsoft [à cette adresse](#).

Danger immédiat

Cette faille se montre exploitable dès sa découverte (d'où le qualificatif de vulnérabilité zero-day). Des attaques seraient d'ailleurs d'ores et déjà en cours au Moyen-Orient et en Asie. Des fichiers Word infectés sont à l'heure actuelle le vecteur d'infection privilégié par les pirates.

La faille permet de prendre le contrôle de la machine d'un utilisateur à distance, avec les mêmes privilèges que ceux du compte piraté (bref, les droits administrateur dans la plupart des cas).

Microsoft précise toutefois qu'une action de la part de l'utilisateur (ouverture d'un document ou d'une pièce jointe) sera nécessaire pour infecter la machine. Cette faille n'est en effet pas exploitable de façon automatisée.

Crédit photo : © Pavel Ignatov – shutterstock

Voir aussi

[Quiz Silicon.fr – 10 questions sur Office 2013](#)

Les nouveautés essentielles d'Office 2013 en images