33 failles chez Microsoft : le Patch Tuesday de tous les records

Pour ses rustines de sécurité, le géant Microsoft édite un correctif record en couvrant pas moins de **33 vulnérabilités avec 13 bulletins.** Toutes les versions des OS de Windows sont concernées, même Windows 7, au même titre que d'autres outils tels que **Internet Explorer**, **Silverlight** ou encore Microsoft Office.

A la loupe, 8 bulletins sont qualifiés de critiques, les autres étant classifiés comme « importants ». Ainsi la mise à jour **MS09-050** corrige trois vulnérabilités dans **Server Message Block Version 2** (SMBv2). Ces failles affectaient le protocole de partage de fichiers et d'imprimantes ainsi que le module **FTP** présent dans les anciennes versions du serveur Web Internet Information Services (**IIS**).

Deux patchs sont réservés à**Windows Media Runtime et lecteur Windows Media** . Cette dernière pourrait permettre l'exécution de code à distance si un fichier ASF spécialement conçu était lu à l'aide du lecteur Windows Media 6.4.

De même, quatre vulnérabilités présentes dans Internet Explorer sont comblées avec le **MS09-054**, qui empêchent l'exécution de code à distance si un utilisateur affichait une page Web spécialement conçue à l'aide d'Internet Explorer.

Concernant Windows 7, le nouvel OS de la firme de Redmond fait son baptême du feu puisque le patch **MS09-061** y fait mention pour des vulnérabilités dans .NET Framework et Silverlight. Ces failles permettent l'exécution de code à distance sur un système client si un utilisateur affiche une page Web utilisant un navigateur pouvant exécuter des applications du **navigateur XAML** (XBAP) ou des applications Silverlight.

Enfin, dernier bulletin critique, celui découvert par Marsu Pilami (sic) de Verisign, le **MS09-062** couvre plusieurs vulnérabilités dans Microsoft Windows GDI+. Elles pourraient permettre l'exécution de code à distance si un utilisateur affichait un fichier image (fichiers BMP, PNG, TIFF ou WMF) spécialement conçu ou s'il visitait un site contenant du code spécialement conçu.

Concernant les bulletins importants, à noter celui découvert par Dan Kaminsky. **MS09-056** corrige deux vulnérabilités dans Windows. Ces vulnérabilités pourraient permettre une usurpation de contenu si un attaquant parvenait à accéder au certificat utilisé par l'utilisateur final pour son authentification.

Enfin et parmi la flopée de patchs, **MS09-058** corrige le noyau Windows des risques de permettre une élévation de privilèges si un attaquant se connectait au système en exécutant une application particulière.

Du gros et du lourd donc chez Microsoft qui dévoile toutes ces innovation sur son site « technique » en français mais aussi en anglais, pour les plus courageux.