Windows 10 : à peine sorti, déjà patché

Officiellement mis sur le marché voici deux semaines, Windows 10 a déjà droit à son premier lot de correctifs de sécurité. Le traditionnel Patch Tuesday de Microsoft renferme en effet pas moins de **4 bulletins de sécurité** qui concernent le nouvel OS. S'y ajoute un patch pour le navigateur Edge, livré avec Windows 10. Le nouvel opus de Redmond occupe donc une place non négligeable dans le Patch Tuesday d'août, la dernière livraison mensuelle des correctifs de sécurité du premier éditeur mondial qui renferme au total 14 patchs. Selon Wolfgang Kandek, le directeur technique de Qualys, 40 % des bulletins génériques affectant de multiples versions de Windows concernent le dernier né des OS de Redmond. Pour Windows 8, cette proportion atteignait les 60 % dans les deux mois qui ont suivi sa sortie.

Considérée comme importante, la faille décrite dans le bulletin MS15-088, qui touche toutes les versions de Windows depuis Vista, permet à un attaquant de récupérer de l'information via un paramètre mal protégé en lignes de commande. Même essaimage à un grand nombre de versions de Windows – dont 10 donc – pour le MS15-085 (élévation de privilèges après insertion d'un périphérique USB vérolé) et le MS15-092 (élévation de privilèges exploitant une faille du framework .Net), renfermant des vulnérabilités considérées comme importantes. Mais le défaut le plus sévère, étiqueté critique donc à corriger d'urgence, touche un composant graphique commun à de multiples logiciels de Microsoft (dont Windows depuis la version Vista, mais aussi Office, Lync et le framework .Net) et permet l'exécution de code à distance en cas d'ouverture d'un document ou d'une page contenant des fontes TrueType ou OpenType particulières (lire le bulletin MS15-080)

Corriger Office, la priorité

La livraison mensuelle de Redmond renferme trois autres bulletins de sécurité critiques, dont celui touchant **le navigateur Edge**. Ce bulletin (MS15-091) révèle que le patch corrige en réalité **4 défauts**, dont les principaux autorisent l'exécution de code à distance via l'affichage de contenus Web spécialement conçus pour infecter la machine. Une fois cette étape franchie, l'assaillant bénéficie des mêmes droits que l'utilisateur ciblé, donc de possibilités multiples s'il est parvenu à convaincre un administrateur de cliquer sur un lien malicieux. A corriger d'urgence donc. Un autre bulletin de sécurité (MS15-079) – associé là encore à un patch corrigeant plusieurs vulnérabilités – concerne l'autre navigateur Web maison, Internet Explorer (version 7 à 11).

Mais, pour Wolfgang Kandek, le directeur technique de Qualys, la « *priorité n°1* » de ce Patch Tuesday réside dans le bulletin MS15-081 touchant Microsoft Office. Il répertorie pas moins de 8 vulnérabilités des versions 2007, 2010 et 2013 de la suite bureautique, dont une, jugée critique, autorise l'exécution de code à distance après ouverture d'un document conçu spécifiquement. Wolfgang Kandek note par ailleurs que le correctif bouche une faille basée sur la corruption de mémoire déjà exploitée par des hackers.

A lire aussi :

Notre dossier : Windows 10, un OS aux multiples facettes

Windows 10 : la mise à jour qui bloque le système

Quiz Silicon.fr – Une semaine de Windows 10