Patch Tuesday de Microsoft : zero days et antivirus corrigés

Microsoft s'est écarté de sa traditionnelle livraison de correctifs de sécurité le deuxième mardi du mois. En effet, la firme de Redmond a corrigé en urgence une faille présente dans le moteur de protection contre les malwares. Hier, nous nous faisions l'écho de la découverte par deux chercheurs du Project Zero de Google d'une vulnérabilité critique au sein de ce moteur. Lorsque ce dernier inspecte des fichiers, il est susceptible de déclencher par erreur le lancement du code malveillant qu'ils peuvent contenir. Menant ainsi à l'infection de la machine. Une menace prise très au sérieux par Microsoft au point de lancer son patch en dehors du Patch Tuesday, quelques heures seulement avant la publication de ce dernier.

Le Patch Tuesday a en effet été dévoilé hier et colmate 57 vulnérabilités. Comme d'habitude, certaines failles sont plus urgentes à corriger pour les administrateurs. Les zero days exploitées en particulier. Le CTO de Qualys livre sur un blog quelques conseils. La priorité dans le catalogue de failles concerne Office, avec la CVE-2017-0261, qui offre la capacité d'ouvrir un fichier Office contenant des images corrompues. Ces documents peuvent être envoyés par email ou par d'autres moyens. Cette vulnérabilité est activement utilisée par les cybercriminels pour pirater des organismes gouvernementaux. Il faut donc la corriger en priorité.

IE et Edge visés par des zero days

Idem pour la CVE-2017-0222, exploitée activement et touchant Internet Explorer. Les cybercrimels peuvent compromettre les utilisateurs en les guidant vers un site infecté et *in fine* prendre le contrôle de leur PC à distance. Le navigateur Edge fait aussi partie des applications à patcher rapidement, notamment en raison de la faille CVE-2017-0229.

Parmi les autres priorités, on note la correction de 3 failles critiques, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279, concernant SMB (Server Message Block). Elles affectent aussi bien les clients serveurs (Windows Server) que les plateformes pour PC.

Flash Player et sus et SHA-1 déprécié

Comme d'habitude, Adobe profite du calendrier de Microsoft pour fournir des patchs pour certains de ses produits. En l'occurrence ici, Flash Player apparaît comme la priorité, avec pas moins de 7 vulnérabilités critiques colmatées.

Enfin, Microsoft a modifié ses navigateurs IE 11 et Edge pour bloquer les sites qui sont protégés avec un certificat SHA-1 soumis à une alerte d'invalidité. Cela concerne les certificats reliés à une racine reconnue par le Microsoft Trusted Root Program (qui valide les certificats émanant d'autorités de certification) continuant à employer l'algorithme obsolète. La firme américaine indique que les certificats SHA-1 édités par les entreprises ne sont pas concernés par cette dépréciation.

A lire aussi :

Adieu Patch Tuesday et bienvenue aux Security Updates

Une faille zero day de Microsoft Office exploitée depuis janvier