Microsoft Patch Tuesday : presque la moitié des vulnérabilités au niveau « critique » en octobre

Les mois se suivent et se ressemblent pour les correctifs de sécurité de **Microsoft**.

Avec son **Security Updates** d'octobre (ex-Patch Tuesday toujours publié le deuxième mardi du mois), la firme de Redmond aligne pas moins de **62 vulnérabilités à corriger.**

Sensiblement moins que les 81 de septembre mais le nombre de failles critiques reste soutenu avec 28 correctifs proposés (contre 27 le mois précédent). Donc la vigilance est de vigueur.

Windows (toutes versions encore supportées confondues, y compris les plates-formes serveurs), Office, les navigateurs Edge et IE et le module de développement ChakraCore sont concernés.

S'il y a une faille à colmater en urgence, c'est peut-être celle référencée CVE-2017-11826. Classée comme seulement « Importante » par Microsoft, elle est actuellement publique et exploitée.

Elle permet à un attaquant d'exécuter les mêmes actions que l'utilisateur victime selon ses droits. Sur un poste d'administrateur, qui dispose de tous les droits, la personne malveillante pourra ainsi prendre le contrôle total du système.

Il faudra préalablement convaincre la cible d'ouvrir un document infectieux, soit en pièce jointe d'un e-mail, soit en cliquant sur un lien de téléchargement ou en se rendant sur une page web spécialement formatée dans ce but.

La vulnérabilité CVE-2017-11771 affecte le service Windows Search. Pour la quatrième fois depuis le début de l'année. Elle ouvre la prise de contrôle du système installé sur les stations de travail comme sur les serveurs.

Et comme précédemment, la vulnérabilité peut être exploitée par le biais de SMB (Server Message Block) utilisé par la NSA pour son exploit EternalBlue et mis au grand jour par le groupe de pirate les Shadow Brokers.

« Bien qu'un exploit contre cette vulnérabilité puisse utiliser SMB comme vecteur d'attaque, ce n'est pas une vulnérabilité dans SMB lui-même, et n'est pas liée aux récentes vulnérabilités SMB exploitées par EternalBlue, WannaCry et Petya », tient à préciser Jimmy Graham de la firme de sécurité Qualys.

Chiffrement défectueux

L'alerte ADV170012 adresse une vulnérabilité dans certains composants TPM (Trusted Platform Module) Infineon chargé d'assurer le chiffrement des données du disque.

Il pourrait en résulter un faible chiffrement des données par BitLocker ou les outils de biométrie, notamment.

Dans la mesure où il ne s'agit pas d'un bug affectant Windows directement mais seulement le composant, une mise à jour du firmware sera nécessaire.

D'ici là, le correctif de Redmond propose une solution de contournement en ajoutant une nouvelle étape d'identification et une option pour utiliser les clés dérivées du logiciel.

Signalons encore la présence de deux brèches dans la bibliothèque de polices (CVE-2017-11762 et CVE-2017-11763) qui peuvent être exploitées depuis le navigateur ou un fichier infectieux.

Fait rare depuis que le Patch Tuesday intègre les correctifs d'Adobe, aucune mise à jour de Flash Player (ou autre) n'accompagne le bulletin mensuel de Microsoft ce mois-ci. C'est peut-être ce qui marque la différence avec le nombre de bulletins de septembre.

Lire également
Windows Server 2003 victime d'un cryptomineur Monero
90% des entreprises attaquées par des failles de plus de 3 ans
Quand un fichier Windows infecte l'environnement Linux

Crédit photo © kalhh via Pixabay