Patch Tuesday Juin 2016 – Data Security Breach

Patch Tuesday Juin 2016

Patch tuesday juin – 16 bulletins de Microsoft pour corriger plus de 40 vulnérabilités pour le mois de juin 2016. Flash souffre d'un 0Day très dangereux.

Le Patch Tuesday juin 2016 arrive avec un cortège de 16 bulletins publiés par Microsoft pour résoudre plus de 40 vulnérabilités (CVE) différentes. Cela porte à 81 le nombre de bulletins pour les 6 premiers mois, ce qui laisse augurer plus de 160 bulletins d'ici fin 2016, un nouveau record pour la dernière décennie en termes de correctifs.
Votre attention doit se porter en priorité sur Adobe Flash. En effet, Adobe a reconnu qu'une vulnérabilité (CVE-2016-4171) au sein du lecteur Flash actuel est en cours d'exploitation en aveugle, si bien que l'éditeur a reporté le patch mensuel pour Adobe Flash. Dans son avis de sécurité APSA16-03. Adobe promet ce patch pour d'ici la fin de la semaine. Surveillez attentivement sa diffusion et déployez-le dès que possible. Si l'outil EMET est installé sur vos systèmes, vous êtes protégés. Pour information, c'est le troisième mois d'affilée qu'une faille 0-Day est découverte dans Flash, ce qui en fait le logiciel certainement le plus ciblé sur les points d'extrémité de votre entreprise.
Ce mois-ci, un ensemble de bulletins à la fois pour les serveurs et les systèmes clients va occuper cette semaine toute l'équipe IT qui devra sécuriser les systèmes de l'entreprise.

Vulnérabilité critique
La vulnérabilité la plus intéressante côté serveur est résolue dans le bulletin MS16-071. Ce dernier corrige une vulnérabilité critique unique sur le serveur DNS de Microsoft. En cas d'exploitation réussie, l'attaquant déclenche une exécution de code à distance (RCE) sur le serveur, ce qui est extrêmement fâcheux pour un service aussi critique que DNS. Les entreprises qui exécutent leur serveur DNS sur la même machine que leur serveur Active Directory doivent être doublement conscientes du danger que représente cette vulnérabilité.
Côté client, la vulnérabilité la plus importante est résolue dans le bulletin MS16-070 Elle corrige plusieurs problèmes dans Microsoft Office. Principale vulnérabilité associée au format Microsoft Word RTF, CVE-2016-0025 déclenche une exécution RCE au profit de l'attaquant. Le format RTF pouvant être utilisé pour attaquer via le volet d'aperçu d'Outlook, la faille peut être déclenchée à l'aide d'un simple email et sans interaction avec l'utilisateur.
Côté navigateur Web, les bulletins MS16-063 pour Internet Explorer, MS16-068 pour Edge et MS16-069 pour Javascript sur Windows Vista traitent plusieurs vulnérabilités RCE critiques qui sont exploitables lors d'une simple navigation sur le Web. Ces vulnérabilités constituent un vecteur d'attaque privilégié pour les cybercriminels et nous vous recommandons de les corriger dans les 7 prochains jours.
Les autres vulnérabilités concernées par ce Patch Tuesday juin sont toutes classées comme importantes. Elles sont généralement exploitées pour élever des privilèges une fois qu'un intrus est parvenu à exécuter du code sur la machine et sont donc associées avec une exécution de code à distance comme décrit ci-dessus. L'exception est MS16-076 qui résout une faille unique dans Windows Netlogon pouvant fournir une exécution RCE à l'attaquant. Sa gravité est moindre qu'une vulnérabilité RCE normale parce l'attaquant devra dans un premier temps prendre le contrôle du serveur Active Directory.

Deux autres vulnérabilités côté serveur dans le patch tuesday juin
Une élévation de privilèges sur le composant du serveur SMB résolue dans le bulletin MS16-075
Une faille dans Microsoft Exchange résolue dans le bulletin MS16-079 entraînant aussi une élévation de privilèges, certains étant liés au patch Oracle dans la bibliothèque Outside-in.
En résumé, il s'agit d'un Patch Tuesday relativement classique mais avec une menace 0-Day connue qui nécessite de surveiller impérativement la publication de la prochaine mise à jour de Flash. Corrigez les autres problèmes en fonction de vos priorités habituelles, mais faites particulièrement attention à la vulnérabilité qui affecte le serveur DNS et qui va forcément susciter des comportements indésirables. (*Wolfgang Kandek, CTO de Qualys).*

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : Patch Tuesday Juin 2016 – Data Security Breach