Microsoft : prêt pour le dernier Patch Tuesday de l'année ?

Sept familles de produits sont concernées par le dernier Security Update (ex-**Patch Tuesday**) de **Microsoft** de l'année 2017 : les navigateurs Internet Explorer et Edge, le moteur de JavaScript ChakraCore de ce dernier, la suite Office et ses déclinaisons en services et applications web, Exchange Server, Malware Protection Engine et, évidemment, l'ensemble des versions de Windows encore supportées (de 7 à 10 en passant par RT 8.1, de Server 2008 SP2 à 2016, en 32 comme 64 bits). Sans oublier le player Flash d'Adobe.

Les correctifs de ce dernier s'intègrent aux 38 mises à jour considérées comme critiques par Microsoft. 21 failles sont classées importantes et une seule modérée (IE 10).

Au total, c'est une soixantaine de correctifs à prendre en main.

32 CVE dont 19 critiques

Un bulletin dans la ligné de celui de novembre, et un peu moins chargé que ceux de septembre et octobre, avec néanmoins 32 vulnérabilités publiques (CVE), dont 19 critiques, et 24 qui corrigent des risques de corruption mémoire. Aucune de ces failles n'est activement exploitée, selon Redmond.

Néanmoins, Qualys recommande d'appliquer en priorité les correctifs propres aux navigateurs dont les moteurs de script font face à des risques de corruption mémoire.

« Nous recommandons d'accorder la priorité aux correctifs des postes de travail pour traiter les 19 mises à jour critiques d'Internet Explorer et d'Edge, car elles sont répertoriées sous la rubrique 'Exploitation plus probable », indique Gill Langston de l'éditeur de sécurité, dans son billet de blog.

« *Il n'y a pas encore d'exploits connus à ce jour, mais c'est une opportunité de conserver l'avance sur les futurs exploits qui pourraient être publiés. »*

S'il y a une mise à jour de Windows à privilégier, c'est celle qui corrige la brèche CVE-2017-11885. Celle-ci ouvre la possibilité d'exécution de code à distance en utilisant RPC (Remote Procedure Call) sur les PC où le Routing and Remote Access Service (RRAS) est activé. Les postes qui n'utilisent pas RRAS sont épargnés.

Correctif des contrôles DDE

Autre recommandation de Qualys : l'application du correctif ADV170021 qui reconfigure les options de contrôle du comportement du protocole DDE (Dynamic Data Exchange) en regard des exploits récemment publiés.

Quant aux CVE-2017-11937 et CVE-2017-11940 qui touchent le Malware Protection Engine et que Microsoft a corrigé en urgence le 7 décembre dernier, elles sont intégrées au bulletin de décembre.

Normalement, le correctif a été automatiquement appliqué aux logiciels qui utilisent le module anti-malware (Defender, Security Essentials, Forefront Endpoint Protection et dans Exchange 2013 et 2016).

Une nouvelle occasion de l'appliquer, si ce n'est pas déjà le cas. Rappelons que la vulnérabilité permet à un fichier infectieux de déclencher, lors d'un scan de sécurité, une corruption mémoire, menant potentiellement à l'exécution de code malveillant.

Microsoft s'apprête donc à terminer l'année de manière relativement sereine sous l'angle de la sécurité. Une accalmie qui est toujours bon à prendre.

Lire également
Microsoft Office affecté d'une vulnérabilité critique vieille de 17 ans
Microsoft Outlook sous la menace d'assauts liés à une vulnérabilité 0-Day
GitHub alerte les développeurs des vulnérabilités dans leur code

(Photo by wocintechchat.com on VisualHunt / CC BY)