Patch Tuesday de septembre : une rentrée chargée pour Microsoft

Pas moins de 81 vulnérabilités sont traitées dans le bulletin de sécurité, le **Security Updates** (ex-Patch Tuesday) de septembre pour Microsoft.

Elles touchent quasiment tout les principaux produits de l'éditeur que ce soit les navigateurs Edge et Internet Explorer (11, 10 et 9), Excel Services, le pack Office, dont Outlook, les plates-formes Windows 10, 8.1 (y compris RT), 7 ainsi que les versions serveurs de l'OS de Redmond (de 2008 à 2016), le framework .NET, Skype… auxquels viennent se greffer les désormais habituels correctifs pour Adobe Flash.

A lui seul, Windows est affecté de 38 failles.

27 failles critiques

Au total, 27 vulnérabilités sont classées comme critiques. Mais 39 permettent d'exécuter du code à distance.

Microsoft souligne par ailleurs qu'une brèche affectant Hololens, son casque de réalité augmentée, est actuellement exploitée.

Parmi cette avalanche de correctifs, les administrateurs devraient accorder la priorité à la vulnérabilité CVE-2017-0161 qui affecte NetBIOS. Exploitée, elle ouvre la voie à une exécution de code à distance sur les serveurs et postes individuels.

Autre priorité à potentiellement privilégier en urgence, la CVE-2017-8686 qui permet la corruption de mémoire du serveur DHCP si ce dernier est en mode basculement (failover).

La faille CVE-2017-8759 est, elle, actuellement exploitée, selon la firme FireEye. Bien que classée parmi les 54 brèches «importantes», elle touche .NET.

« Un attaquant qui exploite avec succès cette vulnérabilité dans un logiciel utilisant le framework .NET peut prendre le contrôle d'un système affecté, indique Microsoft. *Un attaquant pourrait alors installer des programmes; afficher, modifier ou supprimer des données; ou créer de nouveaux comptes avec des droits d'utilisateur complets. »*

L'attaquant devra néanmoins convaincre l'utilisateur d'ouvrir un document infectieux ou une application du même tonneau.

Trois bugs publics

Trois autres bugs, CVE-2017-9417 (qui affecte un composant Broadcom de HoloLens), CVE-2017-8746 (contournement de Device Guard pour injecter du code malveillant dans une session PowerShell), et CVE-2017-8723 (contournement des règles de sécurité dans Edge, une faille

différente de celle récemment publiée par Cisco Talos que Microsoft ne compte pas corriger), sont également publics. Mais apparemment non exploités. Ce qui pourrait ne plus tarder désormais.

Notons enfin que 22 vulnérabilités critiques touchent les navigateurs maison à travers le moteur de script (Scripting Engine). Lequel peut impacter également les applications Office à travers le navigateur (comme les e-mails en premier lieu).

Comme il se doit, il conviendra de mettre à jour les systèmes affectés le plus rapidement possible.

Lire également
Sécurité : le patch tuesday de Microsoft bat des records en juin
Sécurité : Microsoft automatise la recherche de bugs
Windows 10 trop lourd à digérer pour les consommateurs allemands