Sécurité : le patch tuesday de Microsoft bat des records en juin

En parallèle des correctifs exceptionnellement apportés à Windows XP et Server 2003, Microsoft a livré, ce deuxième mardi de juin, son traditionnel patch tuesday de sécurité désormais rebaptisé « Update Tuesday ». Et le moins qu'on puisse dire est qu'il est chargé. Pas moins de 94 brèches sont ainsi comblées. Dont 27 vulnérabilités autorisent des attaques menant au contrôle distant des machines par les assaillants. Soit plus du double environ des bulletins de sécurité publiés ces derniers mois.

Ceux qui appliquent la mise à jour automatique n'ont rien à faire pour protéger leurs environnements. Les administrateurs qui appliquent manuellement les correctifs vont devoir prioriser leurs mises à jour. L'éditeur de sécurité Qualys recommande de se concentrer sur la CVE-2017-8543 qui, selon Microsoft, est actuellement exploitée. *« Les attaquants peuvent prendre le contrôle total de l'ordinateur victime en envoyant une demande SMB au service de recherche Windows »*, prévient Amol Sarwate, directeur du laboratoire des vulnérabilités chez Qualys. Sont visés les Windows Server 2016, 2012, 2012 R2, 2008, 2008 R2 (et 2003) tout comme les versions de bureau Windows 10, 7 et 8.1 (ainsi que XP).

Attaques à la fonte

Une autre vulnérabilité, la CVE-2017-8464 est également exploitée actuellement. Les attaquants peuvent, là aussi, prendre le contrôle des machines ciblées en s'appuyant sur une faille Windows LNK. La encore, l'ensemble des plates-formes Windows, serveurs et desktop, aujourd'hui supportées est concerné par la vulnérabilité. Des failles qu'il convient donc de combler au plus vite.

Moins urgentes mais non négligeables pour autant, les vulnérabilités CVE-2017-8527, CVE-2017-8528 et CVE-2017-0283 exploitent des défauts du moteur de rendu des fontes de Windows pour accéder à sa prise de contrôle. Il faut néanmoins réussir à amener l'utilisateur à visiter une page web spécifiquement infectieuse ou ouvrir un texte Unicode spécialement encodé pour exploiter ces failles.

Office, le vecteur des attaques par ingénierie sociale

Les entreprises utilisant Outlook comme client de messagerie sont avisées de l'existence de la CVE-2017-8507 qui ouvre la voie à la prise de contrôle complète du système à l'ouverture d'un e-mail « contagieux ». Ce même procédé de déclencher une attaque à l'ouverture d'un document Office se retrouve dans les CVE-2017-0260 et CVE-2017-8506. *« Office est un vecteur d'exploitation relativement trivial pour les attaques par ingénierie sociale »*, rappelle Amol Sarwate.

Les navigateurs Edge et Internet Explorer ne sont pas épargnés par ce déluge de correctifs (que l'on retrouvera sur cette page). Ils sont notamment affectés par trois vulnérabilités, les CVE-2017-8498, CVE-2017-8530 et CVE-2017-8523, qui ouvrent la possibilité d'exécuter du code à distance. Elles

sont d'autant plus prioritaires qu'elles sont aujourd'hui publiques même si aucune attaque n'a été signalée par Microsoft à ce jour. Notons enfin que les correctifs des CVE-2017-0291 et CVE-2017-0292 comblent des failles du PDF Windows, là encore pour éviter de l'exécution de code à distance.

Lire également

Microsoft rajoute une option à son Update Tuesday pour les admins
Patch Tuesday de Microsoft : zero days et antivirus corrigés
Plus de vulnérabilités pour Windows 10 que Windows 7 en 2016

crédit photo © drx – Fotolia.com