Microsoft corrige une vieille faille et un bug critique dans SSL/TLS

Entre ShellShock vieille de 18 ans et la vulnérabilité datant de 20 ans découverte dans l'algorithme de Lempel-Ziv-Oberhumer, Microsoft a trouvé une place intermédiaire avec **une faille âgée de 19 ans**. Et elle n'a pas été découverte par l'éditeur, mais par un chercheur d'IBM, **Robert Freeman**. Sur son blog, le spécialiste souligne que la vulnérabilité est identifiée sous le numéro **CVE-2014-6332** avec un fort taux de criticité (9,3 sur 10). Elle touche toutes les versions de Windows depuis au moins Windows 95, via Internet Explorer. La particularité de cette faille et qu'elle est quasi indétectable par les outils actuels de sécurité comme le sandboxing dans IE 11 nommé EPM ou la solution d'atténuation de menaces EMET **(**Enhanced Mitigation Experience Toolkit).

Le chercheur explique être remonté jusqu'à **Windows 95** dans ses travaux, car la version 3 d'IE a intégré VisualBasic Script, porte d'entrée de l'attaque. Il constate que pendant plus de 18 ans cette faille était présente à la vue de tous malgré des correctifs fréquents d'autres bugs dans la même bibliothèque (OleAuth32). Pour réaliser son attaque, Robert Freeman a travaillé sur la **modification de VBScript** à travers des variantes types. Cette manipulation de données est complexe à réaliser prévient le spécialiste. Il craint néanmoins que ce procédé de manipulation des données ne se développe chez les cybercriminels. Il convient donc d'appliquer le Patch Tuesday de novembre qui ne corrige cependant pas les versions de Windows antérieures à Vista.

Une faille également critique dans SChannelSecure

Un malheur n'arrivant jamais seul, Microsoft a profité de son Patch Tuesday de novembre pour colmater une autre vulnérabilité sous le nom de code MS14-066. Cette faille touche le module d'implémentation des protocoles de chiffrement TLS/SSL et **Secure Channel (SChannel)**. En s'appuyant sur ce bug, des attaquants pourraient faciliter l'exécution du code à distance. Pour **Craig Young**, chercheur chez Tripwire, interrogé par nos confrères de *Computerweekly*, « *la liste des produits Microsoft touchés est longue en intégrant les postes de travail via RDP, mais aussi les applications web fonctionnant avec IIS pour HTTPS* ».

Comme d'autres spécialistes, il pousse les administrateurs à installer ce correctif en priorité. **TK Keanini**, CTO de Lancope, précise que ces derniers « *vont avoir deux tâches : la première est d'installer le correctif et réduire la surface d'attaque et la deuxième, plus importante encore, de mettre en place des mesures pour vérifier le réseau pour prévenir ce type d'attaques* ».

Décidément, les protocoles de chiffrement ont quelques soucis de sécurité ces derniers temps. La faille Heartbleed avait jeté le doute sur la bibliothèque OpenSSL. Plus récemment, c'est la découverte de bug dans SSL 3.0 qui a accéléré sa désactivation de plusieurs navigateurs.

A lire aussi :

Nogofail : Google traque les failles de SSL et TLS
5 questions pour comprendre le déchiffrement SSL

Crédit Photo: pixdreams.eu-Shutterstock