Une faille zero day active corrigée en douce par Microsoft

Discrètement, Microsoft a corrigé une faille zero day utilisée par le groupe de cyber-espionnage nommé Zirconium. Cette vulnérabilité, CVE-2017-0005, affecte le composant Windows Win32k dans le GDI (Graphics Device Interface) et touche toutes les versions du système d'exploitation Windows. A noter que malgré le ciblage sur le composant Windows Win32k, l'exploit utilisant la brèche contient du code ciblant l'architecture 64 bits.

Selon Microsoft, une attaque s'appuyant sur cette faille entraîne une corruption de mémoire et une escalade des privilèges, donnant ainsi accès à la machine et à la capacité d'exécuter des codes avec privilèges de niveau administrateur. Les experts de Microsoft disent que les techniques de cette attaque ont déjà été utilisées dans le cadre de Duqu et ont été présentées dans un Bulletin Virus en 2015.

Windows 2000 à 8 ciblés en priorité

La firme de Redmond affirme que cette faille est présente dans toutes les versions de Windows, mais les cybercriminels ont élaboré leur zero day avec application pour s'assurer qu'elle fonctionne sur les PC tournant sur une version de Windows comprise entre Windows 2000 et Windows 8. Pour Microsoft, le fait d'éviter Windows 8.1 et 10 s'explique par l'existence de fonctions de sécurité spécifiques comme des améliorations de l'ASLR, le Supervisor Mode Execution Prevention (SMEP) et la sécurité basée sur la virtualisation (VBS).

Sur la découverte de la faille zero day, Microsoft explique que l'identification a été faite par « un partenaire de confiance », sans donner le nom. Elle a été corrigée dans le bulletin de sécurité MS17-013 publié le 14 mars dernier lors du Patch Tuesday. A cette époque, Microsoft n'avait pas dévoilé la faille CVE-2017-0005, ni que le groupe Zirconium était derrière cette vulnérabilité. L'éditeur fournit une analyse technique de la faille zero day sur son blog d'experts sécurité.

A noter que le bulletin de sécurité MS17-013 corrige également la faille CVE-2017-038 découverte par l'équipe Project Zero de Google et rendue publique avant la livraison d'un correctif.

A lire aussi :

Une faille zero day sur les serveurs Apache massivement exploitée

Comment Windows 10 Anniversary Update a détourné deux attaques zero day

Crédit Photo : Gelbstock-Shutterstock