Microsoft corrige encore Windows Defender en toute discrétion

La semaine dernière, le 24 mai, Microsoft a discrètement corrigé une vulnérabilité critique du composant MsMpEng de Windows. Plus précisément, MsMpEng est un processus de base de Windows Defender, le logiciel anti-malware livré en standard sur Windows 10 et 8.1, et installable sur Windows 7. Découverte le 12 mai dernier par Tavis Ormandy, chercheur en sécurité du Google Zero Project, cette faille autorise l'exécution de programmes non certifiés et donc potentiellement malveillants.

« *MsMpEng comprend un émulateur système x86 complet qui est utilisé pour exécuter des fichiers non fiables qui ressemblent à des programmes exécutables. L'émulateur s'exécute sous la forme NT AUTHORITY\SYSTEM et ne réside pas dans un bac à sable* », explique l'expert sur la page signalant le bug. Et sur laquelle il revient avec moult détails techniques sur le mode d'exploitation de la vulnérabilité.

Cette nouvelle brèche qui touche l'anti-malware de Microsoft est la deuxième que Tavis Ormandy déniche à quelques jours d'intervalle. Le 9 mai dernier, une faille de MsMpEng risquait d'infecter les utilisateurs… qui lançaient une inspection de leur machine à l'aide de l'outil de sécurité. Paradoxalement, les utilisateurs qui avaient désactivé le scan automatique en étaient donc protégés.

Une faille critique facile à exploiter

Le nouveau trou de sécurité s'avère beaucoup plus simple à exploiter selon le chasseur de bugs qui le qualifie de « *vulnérabilité potentiellement extrêmement dangereuse* ». Néanmoins, la brèche avait été reportée de manière privée à l'éditeur de Redmond qui, comme la fois précédente, s'est empressé de la corriger. Pour profiter de cette nouvelle protection, les utilisateurs doivent néanmoins laisser le service de mise à jour automatique activé et s'assurer qu'ils disposent de la dernière version de Windows Defender.

Ce qui n'est pas nécessairement le cas pour les PC en entreprise. Une situation qui pourrait s'avérer d'autant plus problématique que Microsoft n'a apparemment fait aucune communication officielle sur cette vulnérabilité et son correctif. Les cyber-criminels pourraient profiter de l'ignorance des entreprises de l'existence de cette vulnérabilité en particulier (et d'autres plus généralement) pour tenter d'infecter leur SI. Une stratégie qui pousse les organisations à appliquer les mises à jour système au fil de leur disponibilité comme le souhaite Microsoft.

Lire également
Google met à jour une faille zero-day de Windows
Une faille zero day de Microsoft Office exploitée depuis janvier
600 000 serveurs Web Microsoft IIS 6.0 menacés par un exploit zero day

crédit photo : Myriams- via Pixabay