Bug Windows : EnSilo voit un danger potentiel mais pas Microsoft

Toutes les versions de **Windows** – de la version 2000 à celle de dernière génération (Windows 10) – seraient affectées. Un bug de l'OS de Microsoft permet de contourner les logiciels de sécurité et ouvre la porte aux exécutables malveillants.

« Une erreur de programmation dans le noyau Windows pourrait vous empêcher d'identifier quels modules ont été chargés au moment de l'exécution », alerte la firme de sécurité EnSilo sur son blog.

Ce qui revient concrètement à empêcher les antivirus et autres solutions de sécurité de repérer les éventuels codes malveillants en cours d'exécution.

L'origine de l'erreur se trouve dans l'interface du protocole "PsSetLoadImageNotifyRoutine" chargé de notifier le chargement de module en mémoire et potentiellement utilisée par les antivirus.

Dans certains cas, un exécutable malveillant spécialement conçu utilisant cette API pourrait ne pas déclencher d'avertissement.

Du coup, une inspection du système par un logiciel de sécurité sur le PC resterait sans suite. Car les antivirus ont besoin d'être informés du lancement de l'exécution des fichiers pour, si nécessaire, les stopper. Les antivirus qui n'appuient pas leur système d'analyse sur ce mécanisme ne devraient pas être affectés par le bug.

EnSilo a alerté Microsoft de sa découverte. *« Nos ingénieurs ont passé en revue l'information et ont déterminé que cela ne représente pas une menace pour la sécurité et nous ne prévoyons pas de l'aborder avec une mise à jour de sécurité »*, a répondu l'éditeur de Redmond à *ThreadPost*.

De son côté, la firme de sécurité n'en démord pas, il s'agit bien d'une vulnérabilité système aux conséquences potentiellement désastreuses.

Aucune victime en 17 ans

Néanmoins, *« l'attaquant doit d'abord prendre la main sur une machine afin de forcer le système d'exploitation à manifester le bogue »*, déclare le chercheur Omri Misgav à nos confrères américain.

Selon l'expert en sécurité, le bug de PsSetLoadImageNotifyRoutine pourrait être exploité conjointement avec une attaque par injection similaire à Process Hollowing (modification de l'image d'un processus légitime) et AtomBombing.

Cette dernière méthode, qui permet également de contourner les barrières de sécurité, avait déjà été repérée par EnSilo.

Il n'en reste pas moins que, présente de Windows 2000 édité il y a plus de 17 ans, le bug a traversé toutes les versions de l'OS sans qu'aucun éditeur d'antivirus ne s'en plaigne. Soit leurs logiciels de sécurité ne s'appuient pas sur l'API (mais, dans ce cas, pourquoi Microsoft la maintiendrait), soit

aucune attaque l'exploitant n'a jamais été constatée. Ce qui pourrait ne pas durer après les révélations d'EnSilo.

Lire également

Edge est affectée par une faille que Microsoft s'abstient de corriger
Pirater un PC via un code malveillant écrit sur un brin d'ADN
90% des entreprises attaquées par des failles de plus de 3 ans