Sécurité : des PC HP livrés avec un driver audio espion

Un keylogger se serait glissé dans des PC fabriqués par HP. Plus précisément, c'est un pilote audio, fourni par Conexant Système qui intègre une fonction d'enregistrement des frappes au clavier ensuite sauvegardées dans un fichier stocké sur le disque du poste de travail. Un fichier accessible à quiconque saurait où le chercher, administrateur légitime, simple utilisateur où agent malveillant qui aurait pénétré la machine à distance.

La société suisse de sécurité Modzero a alerté Conexant le 28 avril dernier pour l'informer que son driver audio MicTray64 en versions 1.0.0.31 et 1.0.0.42 était affecté de la vulnérabilité référencée CVE-2017-8360. HP a été contacté le 1er mai. Faute de retour efficient des deux entreprises (et particulièrement de Conexant qui semble avoir fait la sourde oreille), Modzero a rendu publique son alerte hier, jeudi 11 mai. La société de sécurité tient à préciser que d'autres fournisseurs de PC que HP pourraient également être impactés par la vulnérabilité dès lors qu'ils embarquent le pilote en question.

Une trentaine de modèles HP affectés

En attendant, près d'une trentaine de modèles HP ProBook, EliteBook, et ZBook sous Windows 7 et 10, en 32 comme 64 bits, ainsi que la version Embedded de l'OS (32 bits), sont affectés par le keylogger. Une vulnérabilité que Modzero considère entre élevé et moyenne. *« N'importe quel framework et processus avec accès à l'API MapViewOfFile est en mesure de capturer en silence des données sensibles en enregistrant les frappes de l'utilisateur »*, assure l'expert en sécurité. Le fichier contenant les données est facilement accessible. Il se trouve dans le répertoire local public (C:\users\public\MicTray.log).

A la connaissance de la firme suisse, aucun correctif officiel n'est à ce jour disponible. A défaut, les chercheurs en sécurité conseillent de déplacer les fichiers problématiques s'ils sont effectivement présents sur le disque. A savoir le fichier d'exécution MicTray64.exe (que l'on trouvera dans le répertoire System32 de Windows) et son fichier d'enregistrement MicTray.log. Et de redémarrer la machine de manière à désactiver le driver. Modzero recommande néanmoins de consulter le contenu du fichier de log afin de vérifier si des mots de passe et autres données sensibles y ont été enregistrée. Auquel cas, il est impératif de les changer sur les comptes associés.

Lire également
IBM livre un malware avec ses systèmes de stockage Storwize
Anatomie du malware super furtif, caché dans la mémoire des serveurs
Le malware bancaire Dridex devient hyper furtif, grâce au AtomBombing