Un logiciel espion dans plus de 400 modèles de PC portables HP

L'information était passée inaperçue. Et pourtant, elle est de taille. *« Les informations contenus dans ce bulletin de sécurité doivent être prises en compte le plus vite possible »*, annonçait HP dans une alerte le 7 novembre dernier.

Sans entrer dans les détails, le constructeur indiquait que *« une vulnérabilité potentielle en matière de sécurité a été identifiée avec certaines versions des pilotes de touchpad Synaptics qui ont un impact sur tous les partenaires OEM de Synaptics. Un intervenant aurait besoin de privilèges administrateurs pour profiter de la vulnérabilité »*.

Notebook, EliteBook, ProBook, Zbook, Envy, Pavilion ou encore des vieux Compaq et des clients légers mobiles, plus de 470 modèles de machines sont affectées. Le constructeur, qui en publie la liste sur cette page, assure que *« ni Synaptics ni HP n'ont accès aux données clients en raison de ce problème »*. C'est déjà ça.

Un malware facilement exploitable

Le problème se matérialise sous forme d'un keylogger, selon le chercheur en sécurité Michael Myng qui a découvert et rapporté la faille plus tôt dans l'année. Autrement dit, un enregistreur de frappes. Le code espion était présent dans le fichier SynTP.sys, livré dans le pilote du pavé tactile Synaptic.

« L'enregistrement était désactivée par défaut mais pouvait être activée en définissant une valeur de registre », indique le chercheur qui détaille sa trouvaille sur sa page postée le 7 décembre.

Un attaquant aurait donc pu exploiter la clé du registre en question pour activer le keylogger et espionner les victimes. Une attaque qui plus est indétectable par les outils de sécurité traditionnels alors que le pilote est signé par le noyau du système d'exploitation.

Un outil de débogage à l'origine

« Le keylogger a sauvegardé les codes de scan dans WPP trace », ajoute Michael Myng. Le WPP tracing est une méthode utilisée par les développeurs à des fins de corrections de bug en cours de développement.

Selon toute vraisemblance, HP aurait donc tout simplement oublié de supprimer ce code utilisé dans un cadre de travail.

Ce n'est pas la première fois que le constructeur fait une telle bourde. En mai dernier, on apprenait que HP avait livré des PC avec un drive audio espion sur le même schéma de code « oublié ».

Outre les correctifs fournis par HP pour chacun de ses modèles affectés, *« la mise à jour est également*

disponible avec Windows Update », assure Michael Myng.

Maintenant que la vulnérabilité est publique, il est urgent de s'assurer que le correctif est appliqué.

Lire également
IBM livre un malware avec ses systèmes de stockage Storwize
Avec Proteus, le malware tout-en-un débarque
Les montres connectées à l'écoute de vos claviers

Photo credit: Christoph Scholz on Visual Hunt / CC BY-SA