Veille technologique EUFI buffer overflow

Les chercheurs en sécurité d'Eclypsium ont découvert une nouvelle vulnérabilité de type "buffer overflow", appelée "UEFICANHAZBUFFEROVERFLOW" et qui est associée à la référence CVE-2024-0762, dans la configuration du module TPM du firmware UEFI, au niveau du sous-système "Mode de gestion du système" (SMM). En utilisant cette fonctionnalité, un pirate informatique pourrait exécuter du code malveillant sur l'appareil vulnérable.

Le firmware UEFI Phoenix SecureScore est employé dans de nombreux ordinateurs équipés d'un processeur Intel. En outre, Phoenix Technologies a fait savoir aux chercheurs qui ont fait cette découverte que ce souci de sécurité touchait "plusieurs versions de son logiciel de firmware. »

De ce fait, et puisque les processeurs Intel sont très populaire, des centaines de modèles sont affecté que se soit chez lenovo, dell ou acer et même hp plusieurs génération de processeurs Intel sont directement associé a cette défaillance .

La vulnérabilité "UEFICANHAZBUFFEROVERFLOW" (CVE-2024-0762) découverte par les chercheurs en sécurité d'Eclypsium affecte le module TPM du firmware UEFI au niveau du sous-système SMM, permettant à des pirates d'exécuter du code malveillant. Ce problème touche de nombreuses versions du firmware Phoenix SecureScore utilisé sur des ordinateurs équipés de processeurs Intel, et par conséquent, des centaines de modèles de marques comme Lenovo, Dell, Acer, et HP sont vulnérables, ce qui nous ammène a poser des questions sérieuses de sécurité au sein même de nos appareils sortis d’ usine .

Sources :

https:// https://www.bleepingcomputer.com/news/security/phoenix-uefi-vulnerability-impacts-hundreds-of-intel-pc-models/www.it-connect.fr/faille-securite-uefi-phoenix-pc-intel-cve-2024-0762/