Un attaquant peut prendre le contrôle total d'une machine en 30 secondes seulement, grâce à Intel AMT

korben.info

Les vulns, c'est comme le PAIC Citron. Quand y'en a plus, y'en a encore.

La preuve avec ce problème qui touche les ordinateurs portables équipés d'Intel AMT (Intel's Active Management Technology), une solution que vous avez peut-être sur votre machine qui permet de faire du monitoring et de la maintenance à distance. Un attaquant peut via un accès physique à l'ordinateur, le booter ou le rebooter tout en appuyant sur le jeu de touche CTRL+P pour accéder au MEBx (Intel Management Engine BIOS Extension) à l'aide du mot de passe par défaut "admin" (AH AH AH), changer ensuite ce mot de passe et activer l'accès à distance sans utilisateur. Cette méthode permet de déjouer les mots de passe BIOS, chiffrements Bitlocker et autres codes PIN mis en place par les admins.

Cela permet ensuite au cybercriminel d'accéder à l'ordinateur via le réseau local (ou à distance via un mécanisme de rebonds sur un serveur tiers) sans avoir besoin d'un mot de passe de session.

Alors oui, il faut un accès physique à la machine, mais sa rapidité d'exécution (reboot, CTRL-P, check check reboot, soit environ 30 sec.) en fait une attaque à prendre au sérieux. Il suffit que vous ayez le dos tourné quelques minutes pour que l'accès à distance soit activé à votre insu. Dans un cadre professionnel, cela peut aussi offrir à un cybercriminel, un accès de choix au réseau privé une entreprise via le VPN en place sur la machine piratée.

Ce sont les chercheurs de F-Secure qui sont tombés sur ce problème.

Intel a pas mal communiqué sur le problème auprès des fabricants de PC en leur demandant d'exiger le mot de passe BIOS pour accéder à Intel AMT, mais malheureusement, ces recommandations sont encore trop peu suivies. Si vous êtes une société, mettez un mot de passe costaud sur AMT et si vous le pouvez désactivez la fonctionnalité. Si un mot de passe est déjà en place et que ce n'est pas "admin", considérez la machine comme hautement suspecte.

Et si vous êtes un utilisateur avec un ordinateur équipe d'AMT, rapprochez-vous de votre service informatique, ou si c'est votre propre machine, mettez-vous aussi un mot de passe costaud à AMT et désactivez-le. Et surtout, ne laissez jamais votre ordinateur sans surveillance dans un lieu public. J'en vois tous les mois qui font ça, notamment dans le train...

Source