Intel corrige une faille sur les puces serveurs commercialisées depuis 2008

Aux âmes bien nées, la valeur n'attend pas le nombre des années. Et la criticité non plus pourrait-on ajouter à propos d'Intel. En effet, le fondeur de Santa Clara vient de publier une série de correctifs qui colmate une faille critique dans le logiciel Management Engine (ME). Ce bug autorise l'exécution de code à distance. Il affecte plusieurs fonctionnalités de Management Engine, comme Active Mangement Technology (AMT), Intel Standard Manageability (ISM) et Small Business Technology (SBT).

L'ensemble de ces fonctionnalités donne à l'administrateur système la capacité de gérer des postes de travail à distance, via les ports 16992 et 16993. A noter que ces fonctions ne se trouvent pas dans les puces pour le grand public, mais dans les processeurs pour serveur et station de travail à destination des entreprises.

Toutes les puces serveurs depuis 2008

Là où le bât blesse, c'est que cette faille touche les puces pour serveur livrées depuis 2008. Concrètement, la vulnérabilité, classée CVE-2017-5689 a été découverte en mars dernier par le chercheur de sécurité de la société Embedi, Maksim Malyutin. En terme de gravité, elle affiche un score de 9,3 sur 10. Elle affecte le microprogramme d'Intel dans les versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5 et 11.6. Les itérations avant 6 et après 11.6 ne sont pas concernées. En conséquence, toutes les versions de processeurs pour serveur livrées depuis 2008 sont vulnérables.

Intel a diffusé une alerte de sécurité, une mise à jour du firmware, mais aussi des conseils pour savoir si des stations de travail exécutent les technologies AMT / ISM / SBT. Le fondeur essaye de rassurer en expliquant qu'aucune de ces fonctionnalités ne sont activées par défaut. Un sysadmin doit activer ces services sur le réseau local. Et quand bien même, Intel précise que seules les solutions AMT et ISM sont sensibles à une attaque réseau. Si le serveur ou le poste de travail vulnérable est exposé sur le Net, un attaquant peut se servir des ports 16992 et 16993 pour mener son offensive.

A lire aussi :

Intel plonge en Bourse face à la menace Zen et Ryzen d'AMD

OpenStack : Intel et Rackspace réduisent la voilure