Meltdown et Spectre : des modifications pour les futurs CPU Intel Xeon et Core

Les futurs processeurs d'Intel bénéficieront de nouvelles couches de protections au niveau du silicium afin de réduire leur exposition aux failles Spectre et Meltdown. On parle là des prochains CPU Intel Xeon, nom de code « Cascade Lake », et Core i de 8ème génération prévus pour le second semestre 2018.

Un partitionnement au niveau silicium

Brian Krzanich, le P-DG de la firme de Santa Clara, explique cela dans un billet de blog. Ces prochains processeurs bénéficieront du « *partitionnement* ». Il s'agit d'ériger des « *« murs de protection » supplémentaires entre les applications et les niveaux de privilèges pour créer un obstacle* ».

Les détails exacts derrière ces «murs protecteurs», comme les décrit Brian Krzanich, restent encore flous. Une des possibilités est peut-être qu'Intel a implémenté au niveau même du silicium les mêmes correctifs logiciels que le groupe a développés.

Ces modifications au niveau du design des puces doivent permettre de lutter contre les variantes Spectre 2 et Meltdown 3 des failles découvertes en juin 2017 par Google Project Zero, l'équipe de Google chargée de traquer les vulnérabilités dites « zero-day ». A noter que des correctifs seront toutefois toujours nécessaires pour lutter contre les vulnérabilités découlant de Spectre 1.

Pour rappel, les failles Meltdown et Spectre ont pour particularité de ne pas être liées à des failles au niveau du logiciel mais à des vulnérabilités matérielles présentes dans la plupart des processeurs commercialisées ces 20 dernières années.

Un pirate peut compromettre la mémoire privilégiée des CPU et de ce fait prendre le contrôle de diverses applications logicielles.

Des correctifs par firmware pour 100% des CPU des 5 dernières années

Les propriétaires de processeurs Intel existants devront, eux, compter sur les mises à jour du microprogramme pour lutter contre Spectre et Meltdown. Cela peut malheureusement se traduire par une dégradation des performances.

En revanche, les modifications apportées aux futurs processeurs Intel ne devraient pas impacter les performances : « *Notre objectif est d'offrir non seulement la meilleure performance, mais aussi la meilleure performance sécurisée.* »

Parallèlement, Intel annonce que les mises à jour par micrologiciel (firmware) sont désormais disponibles pour 100 % de ses produits lancés au cours des cinq dernières années. « *Nous avons*

publié des mises à jour de microcodes pour 100% des produits Intel lancés au cours des cinq dernières années et qui nécessitent une protection contre les vulnérabilités par la méthode de canal latéral découvertes par Google. »

Intel avait largement critiqué pour avoir minimisé l'impact des failles Meltdown et Spectre. La firme, tout comme d'autres acteurs IT tels qu'Apple, avait d'ailleurs été sommée de s'expliquer sur le sujet par un membre du Congrès américain.

Le groupe fait aussi l'objet de quelques 35 plaintes, dont 30 en recours collectifs (class action).

(Crédit photo : Photo by LoKan Sardari on Visualhunt / CC BY-NC-SA)