Meltdown et Spectre : Intel sous pression cherche à rassurer

Face à la déferlante des révélations associées aux failles de processeurs (Meltdown et Spectre), **Intel** doit apporter des éléments de réponse pour rassurer les consommateurs et plus globalement l'écosystème numérique au regard de l'alerte brûlante qui a éclaté en début d'année.

Le leader mondial des puces pour ordinateur fixé quelques échéances de réactualisation et fournit des explications de contexte dans un espace dédié sur son site Internet.

Tout d'abord, la firme technologique, dirigée par Brian Krzanich, assure avoir réalisé des progrès importants dans les correctifs software et firmware à déployer. Une réactualisation globale qui va porter sur les puces conçues par Intel depuis 2012 pour les ordinateurs personnels et les serveurs.

« D'ici la fin de la semaine prochaine, Intel sera en mesure de diffuser des correctifs portant sur 90% des processeurs lancés au cours des cinq dernières années », assure le groupe technologique. La liste des processeurs concernés est vaste (disponible ici).

Parallèlement, les éditeurs de systèmes d'exploitation comme Microsoft, les fournisseurs de plateformes Cloud et les fabricants de terminaux numériques procéderont de leur côté à des réactualisations progressivement.

D'autres fabricants ou concepteurs de puces comme AMD ou ARM sont également concernés par ce vent de mobilisation au regard des risques d'attaques portant les noms de Meltdown et Spectre et susceptibles de favoriser le vol d'information sensibles portant sur l'exploitation de systèmes.

Sur son espace FAQ dédié, Intel explique que ces « exploits » (failles non colmatées par les éditeurs) peuvent engendrer des attaques par canaux auxiliaires (« side channel attacks »). Des attaques particulières qui utilisent les propriétés physique d'un composant ou d'un microprocesseur permettant de contourner les dispositif de sécurité (comme le chiffrement) et de dérober des informations sensibles.

Intel refuse de parler de « bug hardware » ou de failles uniquement associées à ses familles de processeurs alors que la sécurité même des kernels de ses composants est compromise.

« Ces nouveaux 'exploits' influent sur les données associées à l'opération intrinsèque des techniques d'exploitation communes à toutes les plateformes informatiques modernes. Elles peuvent compromettre la sécurité même si un système fonctionne exactement comme prévu dans sa conception. »

Intel assure qu'il a été informé par le collectif de chercheurs tiers des « exploits » Meltdown et Spectre en juin 2017 (Google Project Zero est le principal contributeur des découvertes réalisées).

Depuis, ses propres équipes de recherche et de sécurité auraient entamé des phases de vérification des problématiques soumises, de consultation et de développement de patches adaptés avec le vaste écosystème du groupe.

Mais la recherche d’une réponse globale satisfaisante à toutes les parties concernées est loin d’être évidente à ce stade.

(Crédit photo : Intel)