Foreshadow : de nouvelles failles de sécurité affectent les CPU Intel

Après Meltdown et Spectre, des chercheurs en sécurité ont découvert un nouvel ensemble de failles touchant les processeurs signés Intel et baptisées Foreshadow.

L'exécution spéculative ciblée

Potentiellement, ces failles peuvent permettre à des hackers de dérober des informations stockées sur des ordinateurs.

Intel a été informé du problème le 3 janvier 2018. La firme de Santa Clara a ensuite identifié deux variantes étroitement liées baptisées Foreshadow-Next Generation (NG).

Cette nouvelle classe de vulnérabilités affecte le canal latéral d'exécution spéculative et a été baptisée « L1 Terminal Fault » (L1TF) par Intel.

Ces vulnérabilités concernent la technologie SGX (Software Guard Extensions) d'Intel. Cette dernière a été conçue pour permettre aux applications exécutées sur un ordinateur de placer les données utilisateurs les plus sensibles dans une forteresse virtuelle.

Des mises à jour de sécurité

Les données à l'intérieur de chaque enclave sont censées être protégées contre les modifications ou les accès provenant de programmes externes tels que les logiciels malveillants, ce qui en fait un lieu idéal pour stocker des informations telles que les numéros de cartes de crédit ou de sécurité sociale.

SGX est une fonctionnalité incluse dans les processeurs Core de 7ème génération et plus, ainsi que la génération Xeon correspondante.

Deux variantes de L1TF peuvent être jugulées avec les mises à jour rendues disponibles par Intel. Mais, la troisième, qui ne concerne qu'un sous-ensemble d'utilisateurs – tels que certains data centers – pourrait nécessiter des mesures supplémentaires.

Intel affirme par ailleurs que les failles L1TF sont corrigées au niveau matériel avec Cascade Lake, une future puce Xeon, ainsi que les futurs processeurs Intel Core qui devraient être lancés plus tard cette année.

Vidéo signée Intel :

(Crédit photo : @Intel)