AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

La faille critique ZombieLoad

Contenu

I. Contexte

Après Spectre et Meltdown, voici ZombieLoad, la menace révélée récemment par des chercheurs. Tout le monde est concerné, que ce soit les machines Windows, les serveurs sous Linux, les Mac, les Chromebook, etc… Des centaines de millions d'ordinateurs de par le monde sont concernés par cette vulnérabilité critique touchant quasiment l'ensemble des processeurs Intel fabriqués depuis 2011. Cette fois cependant, seuls les processeurs Intel sont touchés, alors que Spectre visait également AMD et Arm.

Baptisée, selon ses variantes, ZombieLoad, Fallout ou encore RIDL elle fait revivre à Intel le cauchemar des failles Spectre et Meltodown, s'agissant d'une énième vulnérabilité matérielle permettant à un cybercriminel d'accéder à des données traitées par le processeur via des programmes installés sur les machines des victimes potentielles. Les chercheurs ne savent pas si la faille est exploitée par des cybercriminels à ce jour (aucune attaque n'a été rapportée) !

II. Fonctionnement

Les puces Intel présentent une nouvelle faille qui pourrait permettre à des pirates informatiques expérimentés d'extraire des informations sensibles des microprocesseurs. ZombieLoad est une attaque par canal auxiliaire exploitant les techniques d'exécution spéculative. Celles-ci visent à accélérer les processeurs, qui tentent de deviner l'action à effectuer après une commande, en spéculant sur la nature de cette action. Les correctifs sont déjà en cours de déploiement un peu partout mais malheureusement, la performance des processeurs va être réduite…

Le souci réside dans le mécanisme d'exécution spéculative, destiné à maximiser l'utilisation CPU. Il consiste à lancer des instructions de manière anticipée (typiquement, un saut conditionné à des valeurs non encore calculées). Lorsque les prédictions se révèlent fausses, le processeur doit effectuer un retour en arrière, Meltdown intervient à ce moment-là, pour permettre la récupération de données résidant en mémoire. ZombieLoad aussi, mais l'interception est faite au niveau des cœurs logiques des processeurs.

ZombieLoad ou la logique des cœurs

Chez Intel, l'implémentation de cette technologie se nomme Hyper-Threading. Elle permet d'optimiser l'utilisation du CPU en exécutant deux tâches en parallèle sur un même cœur physique. ZombieLoad exploite le fait que le sous-système mémoire est partagé entre les cœurs logiques. Un programme peut, par ce biais, accéder aux données traitées par un autre programme résidant sur le même cœur physique. La nature de la faille fait qu'elle touche l'ensemble des systèmes d'exploitation et des hyperviseurs. Les machines virtuelles n'apportent donc pas de protection. Il est même possible de passer outre les enclaves (régions de mémoire privées ; technologie Intel SGX).

III. Mesures de contournement

Pour éviter la panique générale comme lors des dernières failles de ce type, les chercheurs ont cette fois-ci pris les devants et travaillés directement avec les sociétés fournissant les systèmes d'exploitation. Ainsi, des mises à jour de sécurité pour macOS et Windows 10 sont déjà disponibles. Intel, prévenu il y a un mois, a corrigé la faille sur les processeurs vulnérables, à savoir ceux des gammes Xeon, Atom et Knights, ainsi que les puces Broadwell, Sandy Bridge, Skylake, Haswell, Kaby Lake, Coffee Lake, Whiskey Lake et Cascade Lake.

Par contre, Intel a déclaré que les correctifs allaient brider des fonctions de calcul, et par conséquent, faire chuter les performances de 3 à 9 % des machines concernées. Apple évoque quant à lui une baisse impactant jusqu'à 40 % de ses appareils.

IV. Annexes : démonstration d'attaque

Parmi les démonstrations d'attaque rendues publiques, on notera celle qui permet de reconstituer les URL visitées par la victime ou encore de détecter des mots-clés qu'il saisit. La récupération se fait via un logiciel malveillant exécuté sur le même cœur physique que le navigateur ciblé.

https://youtu.be/W1zUaRQU4JI