Actualités

Failles Meltdown et Spectre des processeurs Intel, AMD et ARM

Voici une présentation succincte des failles Meltdown et Spectre rendues publiques en ce début d'année 2018.

Extrait du bulletin d'alerte de l'ANSSI (Agence Nationale de le Sécurité des Système d'Information) :

Multiples vulnérabilités dans des processeurs - Comprendre Meltdown et Spectre et leur impact

L'existence de plusieurs vulnérabilités sur des processeurs couramment utilisés a été rendue publique. Il n'y a pas à ce jour d'exploitation avérée de ces failles de sécurité appelées Meltdown et Spectre. Pour autant, le CERT-FR* recommande d'appliquer l'ensemble des mises à jour proposées. Voici quelques clés de compréhension. Qu'est-ce qu'un processeur ?

Un processeur est un composant indispensable au fonctionnement des ordinateurs, ordiphones, tablettes (etc.) et des programmes qui y sont installés. Ces processeurs sont construits par plusieurs industriels, notamment INTEL, AMD et ARM et couvrent à eux seuls la grande majorité de nos outils électroniques quotidiens. La couche intermédiaire entre les logiciels et le processeur s'appelle le système d'exploitation (par exemple : Windows, MacOS, iOS, Android, etc.).

Que se passe-t-il ?

Liées à des défauts de conception de ces processeurs, les failles de sécurité Spectre et Meltdown pourraient, une fois exploitées, accorder un accès non autorisé à de l'information protégée (mot de passe, identifiants...).

- Ce défaut de conception rend vulnérable tout système d'exploitation utilisant ces processeurs.
- Ces failles ne permettent cependant pas de modifier les informations et aucune exploitation malveillante de ces vulnérabilités n'a été à ce jour avérée.
- Les hébergeurs d'informatique en nuage (cloud).
- Ces prestataires hébergent régulièrement sur un seul serveur physique, utilisant un processeur, les données de plusieurs clients.
- En exploitant la faille, un attaquant peut donc avoir accès à l'intégralité des données en mémoire.

Que dois-je faire ?

- Il est indispensable d'appliquer l'ensemble des mises à jour proposées, en tout premier lieux les navigateurs et les systèmes d'exploitation (Windows, Macos, iOS, Android si possible). C'est l'une des 42 règles du guide d'hygiène informatique.
- Pour les utilisateurs de produits Microsoft il est également important de disposer d'un antivirus à jour ou compatible avec les mises à jour proposées (par exemple celui de Microsoft ou autre antivirus compatible).
- Retrouvez les correctifs disponibles et plus d'information dans le bulletin d'alerte du CERT-FR
- Pour les entreprises où les hébergeurs, il est recommandé de mettre en œuvre les bonnes pratiques de l'ANSSI sur la virtualisation.

Lire aussi

- les actualités de l'ANSSI pour l'administration
- le bulletin d'alerte de l'ANSSI