



Intel avait été averti en mai-juin 2017 déjà du problème affectant la quasi totalité des microprocesseurs.

© 123rf

## TECHNOLOGIE

# La correction des failles dans les puces d'Intel tourne à la catastrophe

Intel, dont la majorité des puces sont affectées par deux failles de sécurité, a dû stopper le déploiement de mises à jour. Ces correctifs ralentissent les ordinateurs jusqu'à 25%

4 minutes de lecture

Technologies sécurité

Anouch Seydtaghia

Publié mercredi 24 janvier 2018 à 22:20, modifié mercredi 24 janvier 2018 à 22:20.

Pour Intel, comme pour des millions de consommateurs, l'affaire des microprocesseurs défectueux s'aggrave. Le fabricant américain vient de presser ses partenaires de ne plus diffuser ses correctifs de sécurité, les effets secondaires étant jugés trop négatifs par rapport aux bénéfices espérés. Malgré tout, les spécialistes conseillent de tout de même effectuer les mises à jour...

L'affaire avait éclaté le 3 janvier, lorsque la société basée à Santa Clara (Californie) admettait que plusieurs de ses microprocesseurs contenaient deux failles, surnommées Spectre et Meltdown. Avec une expertise technique importante, un pirate pourrait prendre le contrôle d'un ordinateur en exploitant ces failles et dérober des mots de passe, par exemple. Après avoir minimisé le problème, Intel promettait, le 4 janvier, la diffusion d'un correctif logiciel d'ici à cinq jours pour 90% de ses processeurs.

### «Comportements imprévisibles»

Mais en début de semaine, Intel faisait machine arrière en pressant ses partenaires de ne plus diffuser ses mises à jour. La multinationale reconnaissait que ces «patches» dégradent la vitesse des ordinateurs de 2 à 25%. Selon un ingénieur de la société de transport Lyft, dont les données tournent dans les centres d'Amazon Web Services, la vitesse avait chuté de 20%. Ce n'est pas tout: Intel expliquait que les correctifs causaient «davantage de redémarrages que prévu» et «d'autres comportements imprévisibles du système», non spécifiés. Ce sont apparemment surtout les serveurs informatiques qui sont touchés.

Mercredi, les fabricants d'ordinateurs Dell et HP annonçaient qu'ils suspendaient immédiatement la diffusion de ces mises à jour. De quoi susciter l'ire de Linus Torvalds, créateur du système Linux: «Ces patches sont complètement pourris. (Les ingénieurs d'Intel) font des choses complètement folles. Ils font des choses qui n'ont pas de sens», écrivait-il sur son site.

#### Abonnez-vous à cette newsletter



Le point éco

**GRATUIT.** Chaque matin 6h, ce qui agite l'économie dans le monde et en Suisse.

[S'INSCRIRE](#) [exemple](#)

### Au courant depuis mai 2017

De son côté, Steven Meyer, directeur de la société de sécurité ZENData, à Genève, estime que le comportement d'Intel «n'est pas professionnel. Ce n'est pas une PME: certes, le problème est complexe, mais la société dispose de moyens très importants. Intel était au courant de cette faille depuis mai-juin 2017 et aurait dû agir avant. Je ne m'explique pas pourquoi les correctifs ont été si peu testés.»

**Lire aussi:** Spectre et Meltdown vous souhaitent une bonne année 2018!

Que faire? Le CERT, l'agence américaine en charge de la cybersécurité, affirmait il y a quelques jours que le seul moyen efficace pour se prémunir des failles était de racheter un nouveau processeur pour sa machine... «Il faudra qu'Intel change l'architecture de son processeur pour ne plus avoir ce problème, mais la dernière version qui vient de sortir intègre cette faille. Donc ce sera au plus tôt en septembre 2018 qu'une nouvelle version sortira», poursuit Steven Meyer. En attendant, le spécialiste recommande de continuer à effectuer les mises à jour de son ordinateur, en se renseignant aussi sur le site de son fabricant. A noter que les puces d'AMD, qui équipent environ 20% des ordinateurs du marché – Intel détenant le solde –, sont aussi touchées par ces failles.

### Des problèmes pires encore

Expert en cybersécurité renommé, l'Américain Bruce Schneier effectuait récemment un constat pessimiste sur son blog. «Le fait que des designers de microprocesseurs ont construit du matériel à risque durant vingt ans ne devrait pas nous surprendre. Ce qui est surprenant, c'est qu'il a fallu vingt ans pour le découvrir. Dans leur course pour créer des ordinateurs plus rapides, ils ne pensaient pas à la sécurité.» Selon Bruce Schneier, «davantage de problèmes vont survenir, et ils seront pires encore. Cette année sera celle des vulnérabilités des microprocesseurs.»

### Le WEF créera un centre en cybersécurité

#### Le sommet de Davos a été l'occasion d'annoncer la mise en place d'un nouvel institut basé à Genève

Le World Economic Forum (WEF) va s'intéresser davantage à la cybersécurité. Mercredi, l'organisation a annoncé la création d'un centre consacré à cette problématique, qui sera établi à Genève. Aucune date n'a été pour l'heure annoncée, ni le nombre de spécialistes qui y travailleront. L'institut fonctionnera de manière autonome et sous les auspices du WEF.

Alois Zwinggi, l'un des responsables du WEF, en sera le directeur. Selon lui, «si nous voulons éviter l'apparition d'une période sombre pour le numérique, nous devons travailler plus dur pour être certains que les bénéfices et le potentiel de la quatrième révolution industrielle seront sûrs pour la société. Le nouvel institut pour la cybersécurité est conçu pour être la première plateforme à s'attaquer aux cyberrisques d'une manière véritablement globale.»

Interpol et BT Group sont deux des partenaires du WEF cités dans le communiqué diffusé mercredi. Le centre aura plusieurs objectifs: consolider les différentes initiatives en cybersécurité du WEF, créer une bibliothèque indépendante des meilleures pratiques dans le cyberspace, aider des partenaires à améliorer leurs connaissances à ce sujet et créer un cadre réglementaire dans ce domaine.

### Conventions de Genève numériques

Parallèlement à cette annonce, la RTS affirmait mercredi que Brad Smith, président de Microsoft, était présent cette semaine à Davos. L'homme, qui a lancé début 2017 l'idée de créer une convention de Genève numérique, devrait s'entretenir ce jeudi avec le conseiller fédéral Ignazio Cassis, selon la RTS. L'idée que la Cité de Calvin abrite de telles conventions fait son chemin depuis plusieurs mois, avec l'appui des autorités de Genève. Le but est de créer une base commune pour éviter ou tout du moins diminuer le nombre de cyberattaques au niveau mondial. **A. S.**

---

Anouch Seydtaghia  
@Anouch

Journaliste éco/finance, spécialisé dans les nouvelles technologies, intéressé par les voitures autonomes, la cybersécurité et les start-up

---

---

Suivez toute l'actualité du Temps sur les réseaux sociaux

[FACEBOOK](#)   [TWITTER](#)   [INSTAGRAM](#)