Forum: Sécurité

Topic: Performances suite mise à jour faille processeur Intel

Subject: Re: Performances suite mise à jour faille processeur Intel

Publié par: Claude

Contribution le : 09/01/2018 16:28:19

Bonjour,
Toute une batterie de tests ici:https://www.techspot.com/article/1554- ... -cpu-performance-windows/

Traduction de la conclusion:

Conclusion, jusqu' à présent

Eh bien, vous l'avez là. Les utilisateurs d'ordinateurs de bureau ont peu à craindre en termes de perte de performance, en particulier les joueurs. Nous n'avons pas encore testé les CPU plus anciens, mais étant donné le type de charge de travail que nous voyons affecté par le correctif, je ne pense pas qu'il y aura un problème avec le matériel de bureau, mais nous vous informerons certainement s'il y en a un.

La réduction des performances de lecture 4K pour les lecteurs NVMe à grande vitesse est une préoccupation et bien que cela ne devrait pas avoir d'impact sur les jeux, toute application qui est sensible à cela pourrait montrer une réduction des performances. Bien sûr, la brève liste des applications que j'ai testées n' a montré aucune réduction réelle de la période de performance.

Le problème reste néanmoins entier et il a un potentiel bien plus grand en ce qui concerne les serveurs. C'est une préoccupation sérieuse pour les centres de données tant du point de vue des performances que de la sécurité. Ce n'est pas notre domaine d'expertise et ce n'est pas notre domaine d'intérêt, alors nous laisserons ce test à ceux qui sont les mieux équipés pour s' y attaquer.

Mise à jour (1/5): Lorsque nous avons testé et publié cet article, le correctif d'urgence Windows 10 était sorti depuis quelques heures et aucune mise à jour de microcode ou de firmware n'était disponible. Pour les ordinateurs portables et les ordinateurs de bureau de marque, cela signifie que vous devez également mettre à jour votre système avec un nouveau firmware qui proviendra de votre OEM respectif. Pour les constructeurs, cela signifie que vous devez attendre une mise à jour du fabricant de votre carte mère.

Au moment d'écrire ces lignes, une poignée d'entreprises ont commencé à offrir ces mises à jour sur certaines de leurs lignes de produits: Dell, Lenovo/ThinkPads, Asus, Microsoft Surface et d'autres. Lorsque notre plateforme de test reçoit une mise à jour du firmware de sécurité, nous prévoyons d'ajouter ces résultats à cet article. Les utilisateurs autour du web ont commencé à afficher des benchmarks de leurs systèmes avec les deux correctifs appliqués et le résultat semble être un peu moins performant que lorsqu'ils avaient seulement appliqué le correctif OS.

Nous comprenons que le correctif Windows et les autres mises à jour de niveau OS ne couvrent qu'un des trois vecteurs connus pour exploiter les failles. La combinaison de l'OS et du firmware devrait couvrir les trois, bien que dans certains scénarios, des correctifs au niveau de l'application devront également être totalement sécurisés. Pour avoir une meilleure compréhension de Meltdown

et Spectre nous vous suggérons de lire notre condensé de ce que vous devez savoir ou lire les livres blancs.

Mise à jour (1/7): Suite à nos tests initiaux, nous examinons la question plus en profondeur en testant un système de bureau patché pour Meltdown (patch niveau OS) et Spectre (mise à jour firmware/BIOS).

Traduit avec www.DeepL.com/Translator

Apparement la mise à jour du Bios concerne Spectre.