Sécurité GPU : NVIDIA patche ses pilotes contre les méfaits de Meltdown et Spectre

Pour protéger les ordinateurs, serveurs et smarphones contre les failles **Meltdown et Spectre** qui affectent les processeur, il faut patcher les systèmes, les logiciels, mais aussi les pilotes hardware.

On parle beaucoup de la vigilance exercée au niveau des CPU mais les **GPU** sont également concernées par ricochet.

Le spécialiste américain NVIDIA a été l'un des premiers à réagir. Il a renforcé ses propres pilotes GPU pour éviter que les cybercriminels s'en servent pour toucher les CPU et dévoiler les secrets des logiciels en cours d'exécution.

Un effort devenu crucial à l'heure où les serveurs embarquent de plus en plus fréquemment des GPU pour accélérer les calculs, l'intelligence artificielle ou animer des bureaux virtualisés.

Le concepteur de circuits graphiques souligne cependant que ses GPU ne sont pas eux-mêmes sensibles aux failles Spectre et Meltdown.

Car les processeurs graphiques n'ont pas recours à l'exécution spéculative c'est à dire des mécanismes d'optimisation d'exécution des programmes que l'on trouve au cœur des processeurs.

Multi-patches à plusieurs niveaux

Depuis qu'elles ont été dévoilées, les failles de sécurité Meltdown et Spectre, découvertes par les chercheurs du Project Zero de Google, font couler beaucoup d'encre.

Elles permettent à des processus d'aller dérober le contenu mémoire d'autres processus sans escalade de privilèges et malgré les isolations mémoire mises en œuvre par le Kernel et le processeur.

Ces failles, qui affectent principalement les processeurs Intel et ARM mais également ceux d'AMD, ne sont pas liées à un bug mais à une conception défaillante de l'exécution spéculative. Autrement dit, la seule véritable parade est de repenser et redessiner les processeurs.

En attendant, il faut se contenter de rustines logicielles imparfaites plutôt destinées à complexifier les attaques qu'à les réparer. Des rustines qui ne sont pas sans impact sur les performances, notamment celles des serveurs fortement virtualisés ou de base de données.

Les deux méthodes d'exploitation connues de la faille Spectre sont les plus complexes à mettre en œuvre par les cybercriminels mais aussi les plus difficiles à contrecarrer.

Elles nécessitent à la fois de patcher les BIOS, les systèmes d'exploitation ainsi que les logiciels les plus critiques (tels que les navigateurs Web) ainsi que les pilotes clés du système.

(Crédit photo : NVIDIA)