Meltdown – Spectre : des bugs dans les patchs !

Face au mouvement de panique des DSI et de toute l'industrie informatique qui a suivi la divulgation des failles **Meltdown et Spectre** liées à l'exploitation de processeurs, les patchs de sécurité publiés ces derniers jours pour les contrecarrer ont-ils été lâchés trop vite et trop tôt ?

La question mérite d'être posée à la lumière des multiples incidents rapportés ces derniers jours.

Dans un premier temps, ce sont les patchs de sécurité publiés en avance de phase par Microsoft dont la diffusion a dû être suspendue. Elle entraînait des écrans bleus et des redémarrages intempestifs des ordinateurs animés par les processeurs AMD.

Dans un second temps, on apprenait en fin de semaine dernière qu'Intel aurait reçu plusieurs rapports de clients sur des redémarrages intempestifs de serveurs après les patchs de BIOS diffusés par le fondeur et ses partenaires en début de semaine. Ces plantages n'affecteraient que les machines équipées de processeurs de génération Haswell et Broadwell.

Le Wall Street Journal rapporte qu'Intel aurait même demandé à ses clients « Cloud » de suspendre pour le moment l'installation des correctifs en attendant les résultats de l'investigation menée par ses équipes. VMware encouragerait même les utilisateurs de Vmware ESXi à revenir à la version précédente des BIOS.

L'univers Linux n'est pas épargné non plus. Canonical a été obligé de produire un second correctif après que le premier diffusé mardi dernier ait empêché certains serveurs de redémarrer. Preuve que, sur cette plateforme aussi, l'affolement a pris le pas sur la fiabilité.

D'autant qu'un nouveau patch dénommé Reptoline (créé par un ingénieur de Google) serait en passe d'incorporer le noyau Linux à la place de correctifs actuels et, contrairement aux tentatives précédentes, il bloquerait Spectre sans engendrer les pertes de performances.

(Crédit photo : Intel)