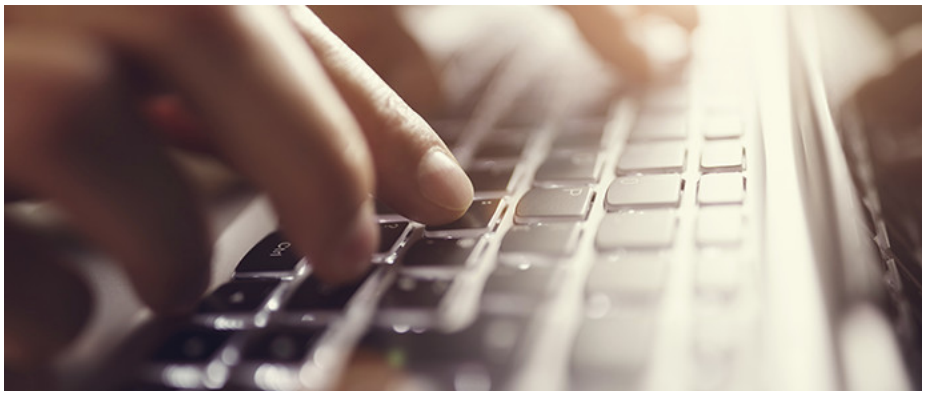
Alerte : Deux failles importantes découvertes. Mettez à jour !



Alerte : Deux failles importantes découvertes. Mettez à jour !

De quoi s'agit-il ? Le 3 janvier 2018, deux failles importantes de sécurité baptisées Meltdown et Spectre ont été révélées publiquement. Ces failles touchent à des niveaux variables les microprocesseurs de la très grande majorité des ordinateurs personnels (PC), mais aussi des serveurs informatiques, des tablettes, des téléphones mobiles (smartphones) dans le monde entier.

Quel est le risque ?

Un attaquant qui parviendrait à exploiter ces failles pourrait avoir accès aux informations personnelles des utilisateurs des machines vulnérables (données personnelles, mots de passe, coordonnées bancaires…).

Ces failles étaient connues depuis quelques mois maintenant des principaux constructeurs de microprocesseurs (Intel, AMD, ARM), des grands éditeurs de logiciels (Microsoft, Apple, Google, Mozilla…) ainsi que des éditeurs d'anti-virus qui préparaient depuis lors des correctifs de sécurité.

Suite aux révélations publiques de ces failles, la manœuvre s'accélère pour les corriger avant que les cybercriminels n'arrivent à en profiter et les premiers correctifs ont commencé à être diffusés.

Etes-vous concernés ?

Certainement. Comme évoqué ci-dessus, la grande majorité des ordinateurs, des tablettes, des téléphones mobile, mais aussi des serveurs dans le monde entier est touchée par ces failles. Ces failles concernent aussi bien les machines qui fonctionnent sous Microsoft Windows, que celles qui fonctionnent sous Apple macOS-iOS, Google Android ou les différentes versions de GNU/Linux.

Que devez-vous faire pour vous protéger ?

Vous assurer de bien installer toutes les mises à jour de sécurité que vous avez peut-être déjà reçues et que vous allez recevoir dans les prochains jours, semaines voire mois des éditeurs de vos systèmes d'exploitation (Microsoft, Apple, Google, GNU/Linux), de vos navigateurs Internet (Microsoft, Google, Mozilla, Apple…), de vos anti-virus.

Pensez à bien vérifier que tous les systèmes de vérification des mises à jour de vos équipements sont bien activés.

Pensez à contrôler également que les mises à jour de sécurité que vous réalisez proviennent bien de vos éditeurs et constructeurs. Des cybercriminels pourraient essayer de profiter de cet événement pour se faire passer pour vos éditeurs ou constructeurs et vous envoyer de fausses mises à jour qui contiendraient un virus. N'acceptez donc par exemple aucune mise à jour que vous recevriez par mail, car c'est une pratique totalement inhabituelle.

Si vous faites vos mises à jour, serez-vous complètement protégés ?

Ce n'est pas complètement certain. Rien ne permet même d'attester que ces failles pourront être intégralement corrigées. Mais les différents correctifs de sécurité qui seront diffusés rendront certainement la tâche bien plus difficile pour les cybercriminels qui voudraient en tirer partie.

Toutes ces mises à jour qui arrivent en même temps peuvent-ils produire des dysfonctionnements de vos matériels ?

Ce n'est pas impossible. Mais le risque de dysfonctionnement est certainement bien moindre que celui de se voir voler ses données personnelles les plus confidentielles (mots de passe, numéros de carte bancaire…) par des cybercriminels.

Vous avez entendu que vos matériels risquaient de ralentir après les mises à jour de sécurité, qu'en est-il ?

Ce n'est pas impossible non plus, mais il est bien trop tôt pour l'affirmer. Vous pouvez même ne pas constater la moindre différence. Quoiqu'il en soit, si tel était le cas, mieux vaut aller un peu moins vite en sécurité, que plus vite en prenant des risques inconsidérés.

Vous avez entendu que ces failles étaient difficilement exploitables, alors devez-vous vraiment en tenir compte ?

Oui, car la cybercriminalité ne cesse de progresser en compétence technique. La vague d'attaques par le rançongiciel (ransomware) Wannacry du printemps 2017 est là pour le rappeler. A peine quelques semaines après la révélation d'une vulnérabilité de haut niveau, les cybercriminels ont réussi à l'exploiter pour une attaque qui a frappé le monde entier.

En conclusion ?

Ces failles sont sérieuses et touchent tous les équipements informatiques ou presque. Il est donc primordial de se sentir concerné et d'appliquer avec sérieux toutes les mises à jour de sécurité officielles que vous recevez de vos constructeurs ou éditeurs

[Original sur cybermalveillance.gouv.fr]

Réagissez à cet article

Source : *Alerte sécurité – Failles Meltdown & Spectre – CYBERMALVEILLANCE.GOUV.FR*