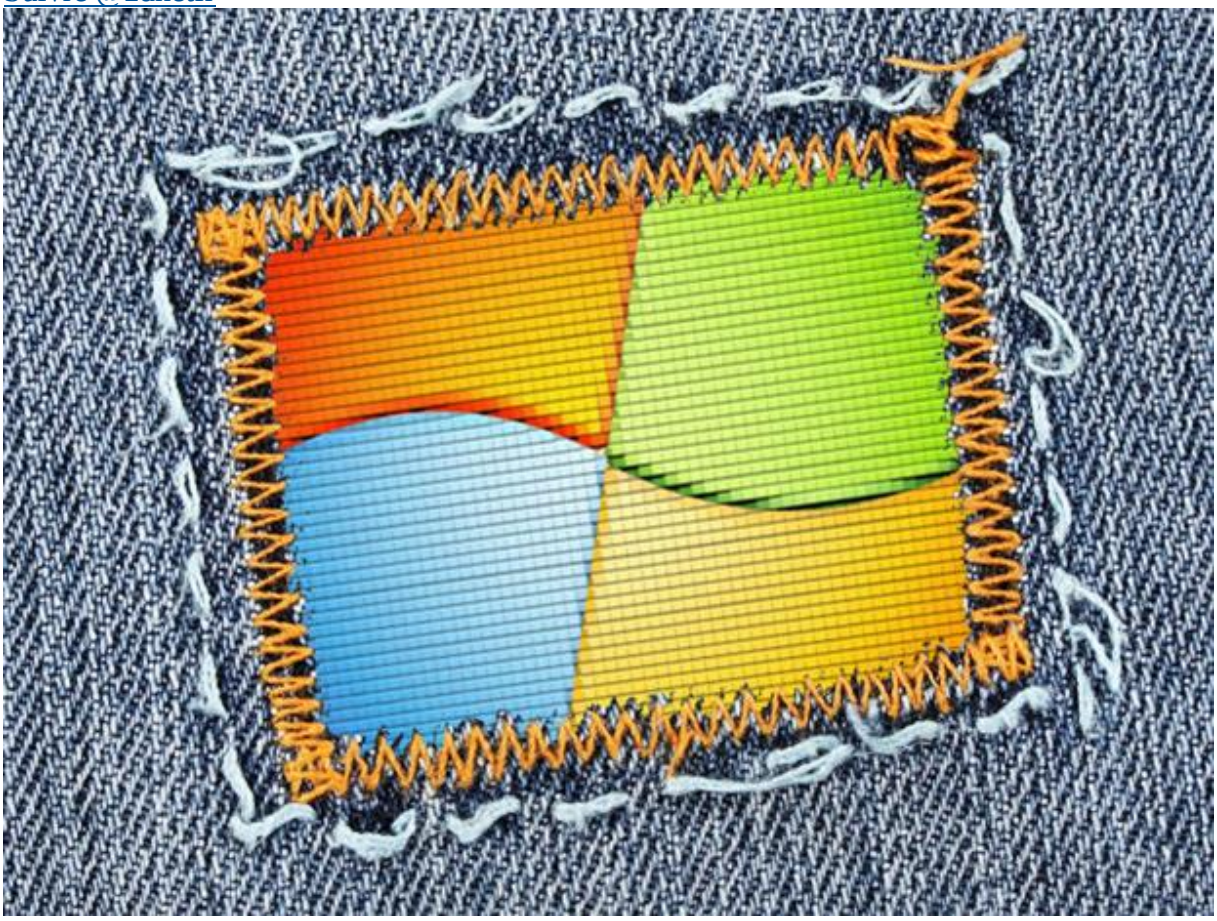
Sécurité des PC Windows : ces logiciels obsolètes vous mettent en danger

Sécurité : *Plus de la moitié des applications installées sur vos PC sont obsolètes - et Windows pourrait aussi avoir besoin d'une mise à jour. Les négligences en matière de mises à jour des applications restent une faille de sécurité très répandue sur PC.*

Par Danny Palmer | Mardi 22 Janvier 2019
Suivre @zdnetfr



Plus de la moitié des applications installées sur les PC Windows sont obsolètes, ce qui peut mettre en danger la sécurité des utilisateurs en raison de failles dans les logiciels déjà corrigés par les fournisseurs.

Environ 55% des logiciels installés sur les PC du monde entier se présentent sous la forme d'une ancienne version de l'application, selon une étude de la société de sécurité Avast - et ce chiffre est en hausse (48%) par rapport à la précédente édition.

15% d'utilisateurs de Windows 7 n'ont pas de correctifs

Basé sur des données anonymisées et agrégées provenant de 163 millions de terminaux dans le monde, le rapport sur les tendances PC d'Avast suggère également que près d'un utilisateur de Windows 7 sur six et un utilisateur de Windows 10 sur dix utilisent des versions non à jour de leur système d'exploitation, ce qui les expose également à une exploitation des failles de sécurité au niveau système.

Certains des programmes les plus souvent laissés obsolètes sont Adobe Shockwave, VLC Media Player, Skype, Java Runtime Environment, et 7-Zip Filemanager.

Repousser l'installation des mises à jour et exécuter des applications obsolètes peut provoquer des bugs et des problèmes d'incompatibilité pour les utilisateurs, mais plus important encore, l'exécution de logiciels obsolètes peut constituer une porte ouverte pour les pirates leur permettant de tirer parti des trous laissés dans les programmes pour lesquels des mises à jour de sécurité critiques n'ont pas été déployées.

Par exemple, il a déjà été constaté que 7-Zip présentait des failles de sécurité permettant aux attaquants distants de lancer des attaques par déni de service, exécution d'un code arbitraire et l'exploitation de vulnérabilités de type "heap overflow". 7-Zip a corrigé les vulnérabilités après leur découverte, mais les utilisateurs qui n'ont pas mis à jour leur logiciel depuis la diffusion du correctif pourraient demeurés exposés à des attaques.

Mises à jour : un classique encore trop négligé

Mais l'obsolescence des applications vulnérables n'est pas la seule source de risques. Un nombre important d'utilisateurs exploitent des systèmes d'exploitation Windows qui n'ont pas reçu les mises à jour de sécurité adéquates.

Windows 7 est toujours utilisé sur des centaines de millions de PC, mais 15% des utilisateurs ne reçoivent aucune mise à jour de sécurité car ils utilisent toujours une préversion de l'OS, souligne notamment Avast.
Par ailleurs, des millions d'utilisateurs exploitent des versions obsolètes du dernier système d'exploitation de Microsoft, Windows 10. Ils s'exposent ainsi à des attaques par le biais de vulnérabilités pourtant corrigées depuis par l'éditeur.
"Nous devons faire plus pour nous assurer que nos terminaux ne nous exposent pas à des risques inutiles" commente Ondrej Vlcek, président d'Avast.

S'assurer que les logiciels et les systèmes sont patchés et mis à jour peut contribuer grandement à protéger les utilisateurs contre les cyberattaques - et leur fournir dans le même temps un PC plus performant et plus facile à utiliser.
Article "PC security warning: That out-of-date software is putting you at risk" traduit et adapté par ZDNet.fr