Microsoft Office serait victime de 3 nouvelles failles

Découverts et annoncés depuis le lundi 9 avril, ces bugs qui touchent encore une fois la suite bureautique Microsoft Office ont fait surface juste avant la publication du bulletin de sécurité de mars de Microsoft corrigeant huit vulnérabilités.

La découverte de ces bugs est à mettre au profit de l'éditeur McAfee. Ces vulnérabilités ont été discutées depuis le début de la semaine sur plusieurs forums spécialisés en sécurité informatique en particulier sur celui de l'éditeur baptisé McAfee Avert Labs blog.

Bilan des courses après avoir testé ces bugs, l'éditeur indique qu'ils provoquent tous un plantage en règle de l'application sous la forme d'un déni de service (DOS).

D'après Karthik Raman, un chercheur de McAfee qui a publié une note sur son blog : *« Il y a une faille dans la façon dont la mémoire est allouée dynamiquement lors de l´exécution d'un programme. Cela permet à un pirate de provoquer un dépassement de tas (Heap Overflow) ou d'exécuter du code malveillant sur le poste cible. »* Reste qu'une attaque Heap Overflow est difficile à lancer et l'attaquant doit remplir un impératif : connaître la nature de l'OS de sa cible.

D'après McAfee, le risque reste réel puisque ce bug peut être exploité en envoyant simplement un fichier contenant du code malveillant à une victime potentielle.

Microsoft a confirmé l'existence de ce trio de bug, mais n'a pour l'instant pas été informé au sujet d'attaques exploitant ces failles. Reste qu'en l'état il n'y a toujours pas de correctif disponible.

Pour Raman :*« Il s'agit encore de failles Zero day publié juste avant le Patch Tuesday, certainement pour maximiser le risque d'exposition à ces vulnérabilités »*. Certains experts de la sécurité parlent avec ironie de *« Zero-day Wednesday »* ou *« faille Zero day du mercredi »*pour mettre en exergue cette étrange simultanéité des découvertes.

Les cybercriminels savent désormais tirer avantage du patch mensuel de Microsoft. Ils ajustent la publication des découvertes de failles avec cette date cruciale pour l'éditeur et ses clients afin d'en optimiser l'impact éventuel.