Alerte : un chercheur découvre une faille dans Vista Windows Mail

Un expert en sécurité affirme avoir découvert une faille dans l'application de messagerie de Windows Vista. Microsoft, informé de cette découverte, déclare avoir lancé une enquête pour en savoir plus. Si le problème est confirmé, un correctif sera publié. Le prochain *« Patch Day »* est prévu pour le 10 avril.

Symantec a décidé de publier une alerte sur cette vulnérabilité.

Rappelons que Windows Mail est le successeur d'Outlook Express, présent dans les OS de la firme depuis Windows 95.

La menace est considérée comme sérieuse: sa note d'alerte a été révisée à la hausse passant, en deux jours de **6.8/10** à **7.5/10.**

Symantec explique avoir découvert que le 'bug' pouvait être contrôlé à distance par un attaquant.

Son fonctionnement est le suivant: dissimulé dans un e-mail, il ouvre un lien vers un site contenant du code.

Une fois que l'internaute a été redirigé, le pirate est en mesure d'utiliser un logiciel de son choix pour récupérer des informations personnelles ou transformer le poste en PC zombie.

Symantec précise que, dans certaines attaques, il n'est pas nécessaire que l'utilisateur visé clique sur le lien pour qu'il s'active et que le poste soit infecté. En effet, le lien URL traditionnellement utilisé par les 'hackers' est un programme exécutable. Le poste est alors immédiatement infecté et de façon quasiment indétectable!

Le réseau de surveillance des menaces de Symantec – DeepSight – précise dans une alerte : *« Le Hacker peut, par exemple, demander l'exécution de winrm.cmd, l'outil de saisie des lignes de commande : Windows Remote Management. «* Cette manipulation lui donne alors le contrôle du poste…

Les équipes du MSRC (*Microsoft's Security Response Center*) estiment que, pour l'heure, le risque est surestimé car la vulnérabilité, non confirmée, n'aurait pas été exploitée.

En attendant, Microsoft, comme Symantec, recommandent aux utilisateurs de Vista de ne pas ouvrir les courriels non sollicités et de désactiver la fonctionnalité HTML dans Windows Mail.