Microsoft Patch Tuesday : un printemps à 6 bulletins de sécurité

Microsoft a publié ses correctifs mensuels de sécurité, hier, mardi 13 mars, dans la soirée. Le *patch tuesday* de mars est traité à travers six bulletins de sécurité dont un est classé « critique », quatre « importants » et un « modéré ».

Les sept vulnérabilités que corrigent les mises à jour concernent les logiciels Windows, Visual Studio, et Expression Design. C'est sur le système d'exploitation que se concentrent la plupart des failles critiques. Vulnérabilité du protocole d'accès au bureau à distance et de la fonction PostMessage, risque de déni de service… De Windows XP à Server 2008 R2, toutes les versions de Windows sont touchées, y compris les éditions serveur, qu'elles aient été installées avec ou sans l'option Server Core, selon les cas.

Windows menacé

Concernant le protocole d'accès distant RDP (inscrit dans le bulletin MS12-020), l'éditeur précise que *« l'ensemble des failles a été dévoilé en coopération avec Microsoft et nous n'avons pas eu connaissance d'exploitation active »*. Un risque moins problématique pour les systèmes qui exploitent l'authentification NLA (*Network Level Authentication*), estime l'entreprise de Redmond qui n'en recommande pas moins d'effectuer la mise à jour dans les plus brefs délais.

Mais face aux délais nécessaires pour tester les mises à jour avant leur application massive sur un parc de machine, Microsoft propose un correctif qui permet d'appliquer l'authentification NLA sans nécessiter le redémarrage du système. Valable pour Vista, Server 2008 et R2, et Windows 7. Une alternative permettant de renforcer la sécurité de Windows en attendant l'application complète du *patch*. On trouvera plus de détails sur la question sur la page du *blog* Security Research and Defense de Microsoft.

Page suivante : les tableaux des risques et priorités d'application des correctifs.