Sécurité : une faille VBScript affecte les versions vieillissantes de Windows

Microsoft alerte d'une **nouvelle vulnérabilité qui frappe Internet Explorer**, toutes versions confondue vraisemblablement. Selon Redmond, une faille liée à VBscript autorise l'exécution de code distant et, donc, le risque de prise de contrôle de la machine affecté. La vulnérabilité en question ne concerne que les environnements Windows 2000 SP4, XP (SP2 et 3 et version 64 bits) et Server 2003. Microsoft confirme que Windows Vista (SP1 et 2), 7 (32 et 64 bits) et Server 2008 R2 (toutes plates-formes confondues) ne sont pas affectés par le bug.

« La vulnérabilité apparaît dans la façon dont VBScript interagit avec les fichiers d'aide de Windows lorsqu'il utilise Internet Explorer, explique l'éditeur dans son alerte. *Si un site malintentionné affiche une boîte de dialogue spécialement conçue et qu'un utilisateur appuie sur la touche F1, du code arbitraire pourrait être exécuté dans le contexte de configuration de la sécurité de l'utilisateur connecté à ce moment. »* Autrement dit, pour être exploitée, **la vulnérabilité nécessite un ensemble de paramètres qui devrait en limiter la propagation**. Microsoft précise d'ailleurs n'avoir constaté aucune attaque sur cette faille en question.

Il n'en reste pas moins une faille actuellement exploitable et non corrigée. Soit une **vulnérabilité dite *« zero day »*** sur laquelle Microsoft déclare travailler à résoudre avec ses partenaires. Il en résultera un correctif livré lors d'un prochain bulletin mensuel de sécurité (le fameux *« patch tuesday »*) ou bien dans le cadre d'une mise à jour immédiate selon l'urgence.

D'ici là, à moins de migrer vers un OS non affecté par la brèche de sécurité, Microsoft propose de **désactiver l'*Active Scripting* du navigateur** en sélectionnant le plus haut niveau de sécurité proposé dans Internet Explorer. Un pis aller qui présente l'inconvénient d'interdire l'accès aux fonctionnalités de certaines pages web…