Firefox 3.6 victime d'une faille 'zero day'

Le jour même où Mozilla corrigeait les failles de Firefox 3.5 et SeaMonkey 2.0, l'expert en sécurité Secunia révélait une vulnérabilité, « ***hautement critique*** », qui affecte cette fois la récente version 3.6 du navigateur open source.

Selon Secunia, bien exploitée cette vulnérabilité peut **compromettre un système** affecté par l'intermédiaire d'injection de code. Le prestataire précise également que la faille peut également affecter les versions antérieures de Firefox. Une faille non corrigée à ce jour et donc **une opportunité pour les pirates de tous poils**.

Secunia rapporte en fait une découverte réalisée en janvier de **Evgeny Legerov**, chercheur russe de la société Intevydis créée en 2008. Dans les faits, il a réalisé un *exploit* pour VulnDisco 9.0, un module de test de sécurité du code utilisé dans le *framework* CANVAS commercialisé par l'entreprise Immunity (dont le forum débat, mollement, de l'existence de la faille). La brèche de sécurité serait exploitable sous Windows XP (SP3) et Vista. Aucune mention de 7, Linux ou Mac OS X n'est indiquée. Dans un Tweet, Evgeny Legerov précise simplement ne pas avoir testé la vulnérabilité sous Windows 7 (et encore moins, suppose-t-on, sur les autres plates-formes).

Si Mozilla ne conteste pas l'existence de la vulnérabilité, l'organisation déclare ne pas avoir réussi à la déceler. « *Mozilla prend toutes les failles de sécurité au sérieux et* ***n'a pas encore pu confirmer la révélation de l'exploit*** », déclare l'éditeur selon des informations rapportées par *The Register*. Mozilla reproche surtout au chercheur de ne pas adhérer à l'usage commun qui veut que les failles soient divulguées publiquement quand un correctif est prêt. « *Nous apprécions les contributions de tous les chercheurs en sécurité et les encourageons à travailler au sein de nos processus de sécurité, à travers une divulgation responsable des vulnérabilités.* »

Ce n'est pas l'avis, ni l'intérêt, de Intevydis qui, en janvier dernier, a décidé de changer sa stratégie en la matière. « *Au fil du temps, notre politique de divulgation responsable a évolué et maintenant nous ne la soutenons plus. Parce qu'elle est appliquée par les éditeurs et qu'elle permet à ces éditeurs d'exploiter gratuitement les recherches en sécurité* », écrit Evgeny Legerov sur son blog. Et de poursuivre : « *Au lieu de perdre votre et notre temps, ne serait-il pas mieux d'allouer des ressources pour faire respecter de bonnes pratiques de codage pour tous vos développeurs amateurs?* » Une manière diplomatique d'annoncer que **le service sera désormais payant**. Une stratégie qui n'a, pour l'heure, pas franchement entraîné l'adhésion des prestataires en sécurité.

A lire également : ***Dossier : quel sera le navigateur phare de l'année 2010 ?***