Le code de Firefox serait plutôt bien écrit. Mais…

Le très populaire navigateur à l'effigie du panda rouge serait d'après des chercheurs en sécurité qui l'ont analysé sous toutes les coutures plutôt bien écrit, mais potentiellement exposé à des menaces.

Un ancien programmeur de la fondation Mozilla s'est empressé de critiquer la méthodologie suivie par le chercheur en sécurité, expliquant : *« cela n'apporte rien et ne devrait pas aider à renforcer la sécurité du navigateur ni résoudre les actuels bugs du programme. »*

Plusieurs versions du logiciel ont été analysées par Adam Harrison de Klocwork par l'intermédiaire de l'outil *« Klocwork's K7 analysis tool*. Cette analyse dont le point culminant a été l'analyse de la version 1.5.0.6 a mis en exergue 611 défauts et 71 bugs potentiels touchant à la sécurité.

Une grande partie de ces bugs s'explique par le fait que le code ne vérifie pas le niveau nul après l'allocation ou la ré-allocation de la mémoire du système.

Les problèmes liés au management de la mémoire vive représentent à eux seuls 141 failles dans le programme. L'échec de la vérification du chemin d'exécution emprunté par le code est aussi fréquemment cité par le chercheur comme une source de bugs.

Les développeurs de Firefox ont reçu ce rapport, que l'auteur lui-même considère comme préliminaire : *« Seuls les utilisateurs disposant d'une connaissance approfondie du code de Firefox peuvent juger du danger d'une vulnérabilité touchant à la sécurité »* déclare le chercheur dans les colonnes du journal *The Register*.

L'on ne connaît pas le nombre exact de failles immédiatement exploitables découvertes par l'outil Klocwork. Et ce, pour des raisons évidentes de sécurité.

Alec Fleet, membre actif et programmeur du projet Mozilla, considère que l'analyse du code source présente certains bénéfices, mais il critique les conclusions de Klocwork qu'il estime incomplète.

« Déclarer qu'il y a 611 défauts dans le navigateur est tout simplement faux. Avec ces outils le pourcentage de faux positif est important » précise Fleet.