Faille ANI : Microsoft fait son mea culpa

L'un des gourous de la sécurité de Redmond explique comment la faille ANI ou « Windows Animated Cursor Handling » est arrivée sur Vista. Michael Howard, une des fortes têtes de l'initiative Microsoft SDL (Security Developpment Life Cycle), qui permet aux développeurs de concevoir du code encore plus sécurisé a publié un long commentaire sur le weblog de la SDL.

Dans cette note, Howard explique les leçons tirées par Microsoft depuis la découverte de cette vulnérabilité et pourquoi ces équipes ont raté le coche.

« La SDL n'est pas parfaite, et elle ne le sera probablement jamais. La découverte de ce bogue montre que nous avons encore beaucoup de travail devant nous » indique Howard.

Cette vulnérabilité ANI, découverte pour la première fois au mois de mars a provoqué un véritable vent de panique chez Microsoft. Preuve en est, l'éditeur est sorti du cadre de son patch day pour publier un correctif. Il faut dire que la faille ANI touchait aussi bien les anciennes versions des OS de Microsoft et la plus récente pourtant *« plus sécurisée »*, Vista.

La réaction de Howard, intervient alors que les chercheurs indépendants émettent de nombreuses critiques à l'égard de l'initiative SDL, *« pour ne pas avoir anticipé la découverte de cette vulnérabilité très critique ».*

Pour eux la tentative de mea culpa de Microsoft n'y change rien, le mal est fait…

Du côté des éditeurs de solutions de sécurité, comme Symantec, le ton est plus modéré et l'on estime que Microsoft a essayé, cette fois au moins, de jouer la transparence en expliquant pourquoi cette vulnérabilité a échappé aux tests préalables à la mise en vente de Vista.

Howard avance une explication. Selon lui, les outils de Microsoft pour le test et le développement de Vista n'ont pas détecté ce bug parce qu'ils utilisent du code qui remonte à Windows 2000 (ndlr: un OS de 7 ans d'age…), une époque à laquelle l'initiative SDL n'existait pas.

Microsoft a donc décidé de jouer la transparence en expliquant pourquoi ces équipes n'ont pas détecté la présence de ce bug. Pour la première fois, l'éditeur de Redmond reconnaît que la détection des vulnérabilités est de plus en plus difficile et qu'il va devoir renforcer ces équipes de sécurité. Il était temps.