

Patch sécurité critique, urgent: Microsoft invite à sécuriser Internet Explorer 'immédiatement'...

Dans un communiqué de ce 17 décembre, envoyé en soirée (20h50), Microsoft France confirme l'invitation lancée à tous les utilisateurs de toutes les versions d'Internet Explorer à télécharger **immédiatement** un 'patch' de sécurité critique, et l'alerte « *La faille non corrigée fait des dégâts* » envoyée il y a plus de 36 heures était bien justifiée...

« *L'éditeur recommande à tous les clients qui utilisent Internet Explorer (IE5, IE6, IE7 et IE8 bêta 2) l'installation immédiate d'une mise à jour corrective qui éliminera tout risque d'utilisation de cette vulnérabilité par d'éventuels vers, virus ou autres malwares.* »

Le communiqué poursuit:

« *Cette mise à jour de sécurité corrige une vulnérabilité du navigateur Internet Microsoft Internet Explorer révélée publiquement. Cette dernière pourrait permettre l'exécution de code à distance si un utilisateur affichait à l'aide d'Internet Explorer une page Web spécialement conçue. Les utilisateurs dont les comptes sont configurés avec des privilèges moins élevés sur le système subiraient moins d'impact que ceux qui possèdent des privilèges d'administrateur* ».

« *Nous recommandons à tous d'appliquer cette mise à jour immédiatement* » .

Comme il se doit, cette mise à jour est disponible sur Windows Update et depuis le site Sécurité : www.microsoft.com/france/securite

Et pour plus d'informations techniques en Français sur cette vulnérabilité <http://www.microsoft.com/france/technet/security/bulletin/ms08-078.msp>.

Bernard Ourghanlian, directeur Technique et Sécurité chez Microsoft France, explique:

« *Nous déplorons que, dans le cas présent, la description de cette vulnérabilité ait été publiée sans laisser le temps à Microsoft d'en fournir le remède* » .

Rappelons que cette vulnérabilité critique a été identifiée par les éditeurs de sécurité le 11 décembre dernier, 24 heures après la publication du dernier bulletin de sécurité mensuel de Microsoft. Pour être exploitée, la faille ne nécessite pas d'interaction de la part de l'utilisateur, la simple visite d'un site Web piégé permet d'infecter sa machine via l'installation discrète d'un cheval de Troie pour ensuite dérober des informations personnelles.

La faille serait liée à la prise en charge de XML par IE dont toutes les versions sont impactées même si la 7 semble particulièrement visée. Elle a été évoquée pour la première fois sur des forums de discussion chinois.

Le 15 décembre, Microsoft indique que la vulnérabilité est largement exploitée sur la Toile, l'éditeur

de sécurité TrendMicro évoque 6.000 sites piégés. Ils seraient 10.000 aujourd'hui.