Failles critiques sur Internet Explorer

Microsoft juge "critique" ce nouveau trou dans son système de navigation. Résultat: c'est de nouveau le patch. Le dernier bulletin de la firme corrige plusieurs failles connues du système de navigation (dans ses versions 5.5 et 6) mais aussi trois nouvelles vulnérabilités...

Et d'une...

La première, réside dans le dispositif d'affichage des pages HTML. Une défaillance existe et permet à un pirate, dans certains cas, d'altérer les informations contenues en tête des pages HTML. En un mot, il est possible de faire croire à IE qu'un fichier en .exe n'en est pas un. Du coup, IE laisse l'internaute ouvrir le dossier sans le prévenir du danger comme c'est normalement le cas pour les fichiers exécutables. Libre au hacker de créer une page HTML qui, une fois ouverte, provoquera l'exécution automatique sur le système de l'utilisateur. Maigre consolation: cette faille n'affecte que IE 6, ce qui n'est pas le cas de la seconde, ni de la troisième.

...et de deux...

Cette autre faille -qui affecte donc IE 5.5 et 6- n'est autre qu'une nouvelle variante d'une faille connue dans "Frame Domain verification" (littéralement une faille dans le système de vérification de la structure du nom de domaine). Plus vicieuse, cette faille permet à un administrateur de site web -de mauvaise intention, il va de soi- d'ouvrir, sur le poste de l'utilisateur, deux fenêtres de navigation Windows. La première n'est autre que celle du site. Plus vicieuse, la seconde s'ouvre sur le fichier local. Les informations transitent alors sans problème du second site vers le premier. Pas de panique: le pirate ne peut que lire les documents privés de l'utilisateur (encore faut-il qu'ils soient explorables à partir d'une page HTML, bien sûr) mais il ne peut y apporter aucune modification.

...et de trois.

Enfin, la troisième et dernière vulnérabilité concerne les boîtes de dialogues. Lorsqu'un fichier est téléchargé depuis le web, une boîte de dialogues apparaît et donne le nom du fichier. Dans certains cas, il est possible pour un pirate, de falsifier l'intitulé du fichier. Inutile de dire qu'il devient tout de suite plus facile de convaincre un internaute de télécharger un fichier infecté. Le problème touche IE 5.5 et 6. Pour Microsoft le risque est critique à tout point de vue: au niveau du client serveur, de l'Internet et de l'Intranet.
Le patch est accessible à l'adresse:
MS

Par Tristane Banon pour :
Silicon

Par

Publié sur Cafeduweb - Archives le dimanche 16 décembre 2001
Consultable en ligne : http://archives.cafeduweb.com/lire/854-failles-critiques-internet-explorer.html