Date de publication Lundi 02 janvier 2006 à 16:54:04 **par** Challenger
Catégorie Nouveautés

Faille Microsoft sur les Fichiers WMF - Attention aux Virus .

TRES IMPORTANT !! FAILLE CRITIQUE ET DANGEREUSE ! Cette énième faille du système d'exploitation vedette de Microsoft se trouve, une fois de plus, dans la gestion des fichiers WMF. Il s'agit ici d'amener un utilisateur à visualiser un fichier WMF trafiqué pour lancer l'exécution de code afin d'infecter un système. Tout au long du week-end du nouvel an de nouvelles variantes exploitant cette faille de sécurité majeure sont apparues et l'on est passé de cinquante à près de soixante-dix déclinaisons que doivent combattre les éditeurs d'antivirus. Divulguée par trois individus, la faille WMF de Windows est massivement exploitée puisque le code source permettant d'en tirer avantage a été publié sur la toile. Profitant de la nouvelle année, l'une des variantes se diffuse au travers d'un email intitulé *Happy New Year* qui contient en pièce jointe un fichier JPG installant en fait une backdoor d'après F-Secure. Toujours d'après F-Secure, les utilisateurs d'Internet Explorer sont potentiellement plus menacés que ceux utilisant des navigateurs alternatifs (Firefox, Opera). En effet alors que l'affichage des fichiers WMF est automatique sous Internet Explorer, l'utilisateur est interrogé sur sa volonté d'afficher un tel fichier avec les navigateurs comme Firefox ou Opera. (Source Clubic) Proposition de Challenger en attendant un patch correctif de Microsoft : Désactivation du composant shimgvw.dll Il apparaît que les applications faisant appel au composant shimgvw.dll de Microsoft Windows deviendraient vulnérables. Parmi les applications vulnérables, nous pouvons citer par exemple Mozilla Firefox, Google Desktop. Cependant cela pourrait avoir des effets de bords sur des applications utilisant cette dll. Les composants de Microsoft Windows affectées par ce contournement provisoire seront au minimum : GDI+ File Thumbnail Extractor Windows Picture and Fax Viewer ; HTML Thumbnail Extractor Windows Picture and Fax Viewer ; Shell Image Data Factory Windows Picture and Fax Viewer ; Shell Image Property Handler Windows Picture and Fax Viewer ; Shell Image Verbs Windows Picture and Fax Viewer ; Summary Info Thumbnail Handler (DOCFILE) Windows Picture and Fax Viewer ; Procédures à suivre : Afin de désactiver le composant shimgvw.dll de Microsoft Windows : Cliquez sur " Démarrer" puis sur "exécuter" ; tapez "regsvr32.exe -u shimgvw.dll" puis "Entrée". Afin de réactiver (lorsque le correctif sera disponible) le composant shimgvw.dll de Microsoft Windows : Cliquez sur " Démarrer" puis sur "exécuter" ; tapez "regsvr32.exe shimgvw.dll" puis " Entrée". Si vous ne disposez pas du fichier regsvr32.exe, il peut être téléchargé à partir du site de Microsoft : ICI Mise à jour au 03 janvier 2006 : Le patch de Microsoft sera normalement disponible pour le mardi 10 janvier 2006 (Le temps que les tests soient terminés) en attendant , restez trés vigilant et mettez vos critères de sécurité de Internet Explorer au Maxi et votre Antivirus à jour !

Billet issu du site internet Colok Traductions:
https://www.colok-traductions.com

URL du billet
https://www.colok-traductions.com/index.php?op=billet&bid=38