

Microsoft alerte sur une énorme faille dans la gestion des DLL

Posté par: tutoriauxpc

Publié le : 26/08/2010 18:13

Microsoft alerte sur une faille dans la gestion des DLL ou plutôt dans la manière dont ces dernières sont appelées lors du lancement d'un programme. Les DLL (Dynamic-Link Library) sont des qui permettent à des programmes de partager du code et d'autres ressources nécessaires pour effectuer des tâches particulières.

Là où le bas blesse, cela concerne des dizaines d'applications comme iTunes, Avast, Firefox pour ne citer qu'eux, c'est quand une application charge une DLL sans spécifier un nom de chemin d'accès complet, Windows tentera de localiser la DLL par la recherche d'un ensemble défini de répertoires.

Il suffit au pirate d'avoir réussi à « glisser » la DLL en question, avec le téléchargement d'un fichier par exemple, et que, quand vous cliquez sur le fichier pour l'ouvrir (un fichier MP3 par exemple) l'application en question ne fasse pas appel au chemin de la DLL, mais à son nom, pour que la faille soit exploitée.

Comme l'explique Microsoft, ces ensembles de répertoires sont connus sous le nom de recherche de chemin d'accès de fichier DLL. Dès que Windows trouve le fichier DLL dans un répertoire, il le chargera. Si Windows ne trouve le fichier DLL dans aucun répertoire dans l'ordre de recherche de fichier DLL, l'opération de chargement de fichier DLL est un échec.

Les fonctions LoadLibrary et LoadLibraryEx sont utilisées pour charger des fichiers DLL de manière dynamique. Voici l'ordre de recherche de fichiers DLL pour ces deux fonctions :

- le répertoire à partir duquel l'application s'est chargée ;
- le répertoire système ;
- le répertoire système 16 bits ;
- le répertoire Windows ;
- le répertoire de travail actuel ;
- les répertoires qui sont répertoriés dans la variable d'environnement PATH.

Le problème comme vous pouvez vous en douter, c'est que plusieurs dizaines d'applications (logiciels) ne se servent pas du chemin absolu pour appeler les DLL au lancement de l'application, mais les appelle par leurs noms.

Alors, attendez-vous dans les prochaines heures / jours à voir « déferler » une vague de mises à jour du côté de vos applications favorites, si ces dernières sont vulnérables.

En attendant, Microsoft propose une rustine temporaire afin de contrôler l'algorithme de recherche de chemin d'accès de fichier DLL :

Une nouvelle entrée de Registre CWDIllegalInDllSearch est disponible pour le contrôle de l'algorithme de recherche de chemin d'accès de fichier DLL

Et surtout, n'oubliez pas de vérifier régulièrement si des mises à jour ne sont pas disponibles pour

vos logiciels, si ces derniers ne vous les proposent pas de manière automatique.