PDF et OpenOffice subissent la menace de failles

Une faille dans ***Acrobat Reader Plug-In*** menace les fichiers PDF. Un bug dans le code d'exécution WMF menace les fichiers ***OpenOffice***. Dans les deux cas l'affaire est jugée sérieuse par les experts en sécurité.

Acrobat Reader Plug-In, une menace pour les fichiers PDF

Dans le cas du PDF, la menace est double : d'une part, comme pour Windows, l'environnement d'Adobe est très largement répandu dans le monde des PC, et plus le nombre d'utilisateurs est important, plus les dégâts peuvent prendre de l'ampleur.

D'autre part, les instructions pour exploiter la faille via les navigateurs Internet Explorer ou Firefox circulent sur internet, et l'on pourrait assister à une multiplication des '*proof of concept*', des modules de tests qui vont tenter de l'exploiter, sans pour autant toujours adopter une démarche mafieuse.

La faille exploite l'échec d'*Acrobat Reader Plug-In* à valider les paramètres URI du code scripté, ce qui permet au script caché de s'exécuter sans qu'il soit nécessaire de se connecter au site web qui héberge le fichier PDF.

L'information a largement était commentée au cours du vingt troisième *Chaos Communication Congress* consacré aux applications Web 2.0. Deux chercheurs, Stefano Di Paola et Giorgio Fedon, ont présenté un document qui expliquait les risques associés à cette faille, et depuis de nombreux chercheurs en sécurité ont démontré la vulnérabilité de la version d'Adobe Reader.

Le passage à Acrobat Reader 8 s'impose donc, et c'est gratuit !

Un bug d'exécution du code WMF dans OpenOffice

Cette seconde menace est prise très au sérieux par les experts en sécurité, et même qualifiée de '*hautement critique*' par Secunia. OpenOffice, alternative libre de la suite bureautioque Office de Microsoft, est vulnérable à un code d'exécution WMF (*Windows Metafile*) détourné.

C'est historiquement la seconde menace sérieuse qui pèse sur OpenOffice, un risque similaire avait été corrigé en mai 2005?

En ouvrant sous OpenOffice un fichier vérolé, l'utilisateur risque de saturer sa mémoire selon la technique du '*buffer overflow*', ce qui si l'attaque est un succès risque de se produire à chaque fois qu'OpenOffice est ouvert.

Dans ce cas, c'est le passage à la version 2.1 d'OpenOffice qui va corriger la faille.