G-Data : Une faille dans les versions Java rÃ©centes installÃ©es dans Windows
Navigateur
PostÃ© par : JerryG
PubliÃ©e le : 14/4/2010 0:00:00

Deux chercheurs ont publiÃ© lâ□□existence dâ□□**une vulnÃ©rabilitÃ© dans le Java Runtime Environment de Sun**.

Il donnerait Ã des attaquants de nouveaux points d'attaque par Drive-by-Download afin de compromettre les systÃ¨mes dâ□□exploitation Windows ainsi que les navigateurs Web les plus populaires. La vulnÃ©rabilitÃ© a Ã©tÃ© Ã©valuÃ©e comme Â« extrÃªmement critique Â» par les experts en sÃ©curitÃ© de **G Data Software.**

Java Ã©tant installÃ© sur beaucoup d'ordinateurs, cette faille pourrait rapidement attirer l'attention des cybercriminels. Facilement exploitable dans la plupart des navigateurs Internet, elle nâ□□est pas bloquÃ©e par les dispositifs de sÃ©curitÃ© de Windows Vista ou Windows 7.

Comment se protÃ©ger ?

DÃ©sactiver le Java-script ne protÃ¨ge pas contre lâ□□exploitation de cette vulnÃ©rabilitÃ©. Actuellement sans information claire de la part de Sun sur la correction de cette faille, G data conseille Ã lâ□□utilisateur de changer manuellement ses configurations logicielles. Pour les deux navigateurs les plus populaires les manipulations ci-dessous permettent de limiter le risque :

- Pour Microsoft Internet Explorer, il est nÃ©cessaire de placer un Bit dâ□□arrÃªt pour lâ□□ActiveX classe ID CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA. Le manuel sur la faÃ§on dont rÃ©aliser cette manipulation peut **Ãªtre consultÃ© ici**

- Pour Mozilla Firefox, ouvrez le menu Outils et choisissez Modules complÃ©mentaires. Dans lâonglet Plugins sÃ©lectionnez Java Deployment Toolkit et cliquez sur DÃ©sactiver.

Les coulisses de la dÃ©couverte

Le chercheur en sÃ©curitÃ© Tavis Ormandy a publiÃ© les informations concernant cette vulnÃ©rabilitÃ© sur seclist.org. La vulnÃ©rabilitÃ© provient du plug-in Java Deployment Toolkit des navigateurs Internet. Il est installÃ© automatiquement avec le Java Runtime Environment depuis la version 6 (release 10) dans les navigateurs Internet comme Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome.

La mÃ©thode dâattaque permet d'exÃ©cuter du code arbitraire Ã lâexÃ©cution du lanceur web Java. Ormandy a publiÃ© une preuve-de-concept qui met en marche la calculatrice dans Microsoft Windows.

Seulement quelques heures plus tard, le chercheur **RubÃ©n Santamarta** publie la faÃ§on de charger un DLL arbitraire Ã distance. Selon Santamarta il est possible de contourner les mesures de sÃ©curitÃ© DEP et ASLR. Le fichier DLL est alors directement chargÃ© dans le processus mÃ©moire du lanceur Web.