# Première faille 2004 pour Microsoft

La vulnérabilité d'Internet Explorer, qui représente la première faille Microsoft de la nouvelle année, n'est pas nouvelle? Il s'agit en effet d'une variation sur le contournement de la zone 'showhelp()'. Elle n'est pas non plus critique. Cependant, aucun 'patch' proposé par Microsoft ne vient à l'heure actuelle la corriger. Les sites Web peuvent appeler la fonction 'showhelp()' pour ouvrir localement un fichier d'aide compressé au format 'CHM'. Ce fichier fait généralement référence aux commandes système et exécute du code avec les privilèges de l'utilisateur. Ce n'est normalement pas une faille, puisque les fichiers 'CHM' sont liés à des applications reconnues et validées, comme WinAmp, XMLHTTP, ADODB ou d'autres, qui en profitent car leur allocation est généralement connue et standardisée. Cependant, l'utilisation d'une syntaxe spécifique, qui reprend un double « : » peut être combinée avec des codes de navigation transversale, comme des séquences de caractères « ..// ». La vulnérabilité d'Internet Explorer 5 et suivants provient donc de la faculté d'exécuter un code arbitraire en profitant d'applications dont l'installation a été réalisée 'par défaut'. La combinaison d'Internet Explorer 6 et de WinAmp 5 l'aurait démontré. En l'absence de 'patch', la solution est soit de désactiver le support 'active scripting', soit de paramétrer les options de filtrage d'un proxy ou d'un firewall afin de bloquer les pages HTML qui font référence à 'showhelp()'. Ou encore d'utiliser un autre navigateur ! Plus d'informations sur Secunia.