Faille critique sur Yahoo Messenger

Le site spécialisé dans la sécurité Secunia met en garde les utilisateurs de Yahoo Messenger (v5.x) contre une faille de sécurité qualifiée d'

« extrêmement critique ». La vulnérabilité, dont l'origine se trouve dans le dépassement de la mémoire tampon, permet à un pirate extérieur d'exécuter des programmes à distance. Pour l'exploiter, il suffit au pirate de faire parvenir un surplus de données à l'outil de dialogue, par exemple sous la forme d'une adresse Internet très longue. Lorsque l'internaute cliquera sur celle-ci (depuis une page web ou directement depuis Yahoo! Messenger), il provoquera dans le meilleur des cas l'arrêt du programme, et sinon l'exécution du code exécutable malicieux que le pirate aura placé à la fin de l'adresse piégée. Après quelques flottements, Yahoo a finalement mis à disposition un patch correctif à cette adresse. Par précaution, au reste, Secunia conseille d'effacer le fichier **yauto.dll** du programme. Il s'agit du contrôle ActiveX fautif, qui n'est pas essentiel au bon fonctionnement de Messenger.