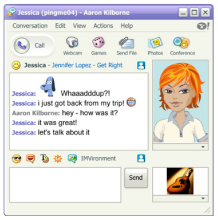
18 July 2007

By: Bogdan Popa, Security and Search Engines Editor



Yahoo Messenger chat window

Yahoo Messenger Still Unpatched, Users at Risk!

A security flaw remains unpatched

The instant messaging created by the Sunnyvale company Yahoo is again vulnerable to attacks but this time, it is even more serious as the firm's engineers left the hole unpatched. Rajesh Sethumadhavan discovered a problem with the Yahoo Messenger address book handling because any malicious entry added to the application can crash the application in a matter of seconds. If you're in doubt that you might have a dangerous address book entry, you can try the following trick: login into Yahoo Messenger, go the address tab in the application and place the mouse cursor over the items placed in the list.If there is any malicious address book entry, the instant messenger should crash, without any chance to recover the information. Of course, the exploitation can be done extremely easy: send a dangerous address to the user and then trick him to place the mouse over the entry. According to the report, a successful exploitation of the flaw might allow the attacker to execute applications with the same privileges as the ones owned by the logged user.This is not the first time when Yahoo Messenger is vulnerable to attacks but recently, the instant messengers were all affected by more or less critical flaws. Take the example of Trillian, an all-in-one instant messenger that allows the users to connect to multiple networks in the same time, including Jabber servers, Yahoo Messenger, MSN and AIM. The security companies discovered some security holes in Trillian that might harm users' computers and make them vulnerable in front of the attacks.Some time ago, it was reported that Yahoo Messenger has become a dangerous program because the hackers are trying to launch phishing attacks using the chat application. Today, a new vulnerability that sustains the same idea is published on the Internet. What's the truth behind those reports? You choose.

Copyright (c) 2001-2009 Softpedia. All rights reserved. Softpedia™ and Softpedia™ logo are registered trademarks of SoftNews NET SRL.