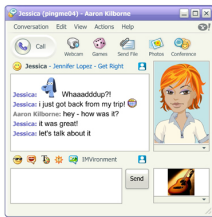


16 August 2007

By: Bogdan Popa, Security and Search Engines Editor



Yahoo Messenger chat window

## [I Simply Love Yahoo Messenger, Especially When It Makes Me Vulnerable!](#)

*And today, I love YM once again*

Yahoo Messenger, the software solution that is regarded by some of the users as the only instant messaging client that deserves to be installed on a computer, contains a critical security hole that might really harm your computer. The vulnerability was first published on a Chinese security forum but the folks from McAfee, one of the largest security firms in the world, analyzed it and provided valuable information for all the Yahoo Messenger fans. First of all, you should know that it affects the webcam support provided by the application so, if you're not one of the ones that love to do live-chatting, then you're free to go. According to McAfee, the only version of Yahoo Messenger affected by the vulnerability is 8.1.0.413 but other versions might be also unsecure in front the attack. The only exploitation technique discovered until now is sending a webcam invite so, the safest solution to avoid the danger is refusing and denying any unknown or untrusted webcam invitation received by you. "It seems like a classic heap overflow which can be triggered when the victim accepts a webcam invite. Note that this vulnerability is different from the recently patched one in June which exploited the Yahoo! Webcam ActiveX controls," McAfee notes. Another solution mentioned by the security company is blocking "outgoing traffic on TCP port 5100 until the vendor patches this vulnerability." "To mitigate this, we're releasing our NIPS IntruShield signatures today to protect Yahoo! Messenger users from this threat. We shall keep on monitoring this threat and update if we come across anything." "So, we're now expecting a new version of Yahoo Messenger to be released in the upcoming days but what's most important is that this is another sign of vulnerability in one of the most popular chatting software solutions available on the Internet.