

Yahoo Instant Messenger Long Filename Downloading Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-01/0214.html>

From: Tri Huynh (trihuynh_at_zeeup.com)

Date: 01/08/04

To: "Tri Huynh" <trihuynh@zeeup.com>, <full-disclosure@lists.netsys.com>, <bugtraq@securityfocus.com>
Date: Thu, 8 Jan 2004 03:38:43 -0800

Yahoo Instant Messenger Long Filename Downloading Buffer Overflow

PROGRAM: Yahoo Instant Messenger (YIM)
HOMEPAGE: <http://messenger.yahoo.com>
VULNERABLE VERSIONS: 5.6.0.1351 and below

DESCRIPTION

YIM is one of the most popular instant messengers. This is a cool product that supports many useful features like audio/video chatting, file transferring...

For more details about the product, please go to <http://messenger.yahoo.com>

DETAILS

By sending a specially crafted long filename to a user, an attacker can cause a buffer overflow when the user's YIM tries to download the file from the server. (No need to run the file).

For a fast demonstration, you can create a file like this "test<insert around 210 spaces here>.jpg" and send it to another user and ask her to download it.

Because this is a buffer overflow, there is always a possibility to run malicious code on the user's machine.

NOTE : This vulnerability is different from the one was discovered by Hat-Squad team in October.

WORKAROUND

Full-Disclosure: Yahoo Instant Messenger Long Filename Downloading Buffer Overflow

Yahoo has been contacted at security@yahoo-inc.com and I got no response except that they said they are looking to it...and here is the interesting story on how

Yahoo handle it (after my little investigation) which I quote from an email I sent

to a friend in the PenetrationGroup about the issue (sorry for my laziness 8-):

"I already contacted Yahoo couple days ago...

.....After reading your email, I removed my YIM and downloaded the new one from their

website and you are right; the newest version 5.6.0.1358 is not vulnerable.

However,

there is NO WAY to upgrade from 5.6.0.xxxx to 5.6.0.1358 except you reinstall

YIM; and of course Yahoo doesn't tell anybody about it either.

If you go to <http://messenger.yahoo.com/messenger/security/> you will see there is

no update for this vulnerability. Again, the only way to patch it is reinstall YIM

which Yahoo doesn't say anything about it.

(FYI, This vulnerability lays in the file ft.dll which is used to handle file transferring in YIM.

They do patch this file in the new version, however if you want to dig more into this thing, you can always get the old file from any of the YIM users you know easily since nobody reinstall their YIM for no reason.)

So here is the new Yahoo! security strategy. Instead of informing the users and

issuing a patch, they slip the patch into their main program silently and say nothing about the vulnerability. Doing so, they can avoid

the press to embarrass them for leaving so many vulnerabilities in their product. However,

it is also a big embarrassment if they protect ONLY new users who download the new version and leave millions of other users who are using the old

version with

no patches available and are uninformed of the vulnerability. Yahoo !.....

"

The only way to patch it is removing and reinstalling YIM from Yahoo website. Don't

waste your time to look for a patch in the messenger security page or any info about this vulnerability

from them. They don't give a damn !

CREDITS

=====

Discovered by Tri Huynh from SentryUnion

DISCLAIMER

=====

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

FEEDBACK

=====

Please send suggestions, updates, and comments to: trihuynh@zeeup.com