

Re: Cross-site Scripting with Local Privilege Vulnerability in Yahoo Messenger

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-01/msg00661.html>

- *From:* "3B.Security Researcher" <3b.maillist@xxxxxxxxxx>
 - *Date:* Sun, 28 Jan 2007 01:13:40 +0530
-

Hi friends,

Bingo! It works on the Y!messenger version 8.1.0.209 and have verified it on my setup.

Quite strange indeed! Good finding ;) Let us see if it can be "really" exploited.

Cheers!

On 1/28/07, Ahmed Sheipani <sheipani@xxxxxxxxxx> wrote:

Hello

I have just tested this with Yahoo! Messenger 8.1.0.209 , and it does not seem to work..

However, I noticed that after setting the FirstName parameter to a very long one, the automatic notification message does not appear anymore.

-----Original Message-----

From: hainamluke@xxxxxxxxxx [<mailto:hainamluke@xxxxxxxxxx>]

Sent: Friday, January 26, 2007 7:27 AM

To: bugtraq@xxxxxxxxxxxxxxxxxxxxxx

Subject: Cross-site Scripting with Local Privilege Vulnerability in Yahoo Messenger

Importance: High

DESCRIPTION:

I've found a cross-site scripting vulnerability in Yahoo! Messenger, a popular advertisement-supported instant messaging client and protocol provided by Yahoo! Attacker can inject a malicious script with local privilege to Y!M notification message.

The vulnerability is discovered in the chat dialog. The automatic notification message of Yahoo! Messenger, for instance "Hai Nam Luke has signed out. (1/26/2007 10:03 PM)" or "Hai Nam Luke has signed back in. (1/26/2007 10:04 PM)" can be easily exploited with injecting a malicious script to. Script is disabled in chat messages but system notification message. That Yahoo Messenger uses Internet Explorer to display messages,

Re: Cross-site Scripting with Local Privilege Vulnerability in Yahoo Messenger

the malicious script will be run with local privilege in the Internet Explorer Temporary Folder. This serious vulnerability could allow attacker gain the victim's system access.

Inject unexpected script also causes other Yahoo! Messenger's errors.

AFFECTED VERSION:

Yahoo! Messenger 8.1.0.29 and previous versions

PROOF OF CONCEPT:

- + Firstname: Hai Nam Luke Hai Nam Luke Hai Nam Luke Hai Nam Luke . (as long as victim cant see the lastname)
- + Lastname:
- + Request to add victim ID to your contact list.
- + Once victim accepts your request, send him a message and change your online status (Available -> Invisible)

This vulnerability was reported to Yahoo!

Hai Nam Luke <hainamluke@xxxxxxxx>
K46A – NEU