

[NT] Multiple Vulnerabilities in Yahoo! Messenger

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0020.html>

From: support@securiteam.com

Date: 06/06/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 6 Jun 2002 07:24:16 +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.

Multiple Vulnerabilities in Yahoo! Messenger

SUMMARY

There are multiple vulnerabilities in Yahoo! Messenger. Attackers that are able to exploit these vulnerabilities may be able to execute arbitrary code with the privileges of the victim user. We have not seen active scanning for these vulnerabilities, nor have we received any reports of these vulnerabilities being exploited, but users should upgrade to version 5,0,0,1065 or later.

This advisory is provided to clear up things regarding the vulnerabilities mentioned in: <http://www.securiteam.com/securitynews/5BP0R2075K.html>>
Yahoo Messenger – Multiple Vulnerabilities.

DETAILS

Systems Affected:

* Yahoo! Messenger version 5,0,0,1064 and prior for Microsoft Windows

Yahoo! Messenger is a widely used program for communicating with other users over the Internet. On May 27, 2002, a buffer overflow and a URL validation vulnerability were discovered in the Yahoo! Messenger client for Microsoft Windows. Details of each vulnerability follow:

Securiteam: [NT] Multiple Vulnerabilities in Yahoo! Messenger

Yahoo! Messenger contains a buffer overflow in the URI handler. The buffer overflow occurs during the processing of the Yahoo! Messenger URI handler (ymsgr:). This URI handler is installed at the system level for applications that use the underlying operating system when processing URIs (such as Microsoft Internet Explorer, Netscape Navigator 6, Microsoft Outlook, or the command shell). A URI can be sent by another Yahoo! Messenger user in a message, embedded in a web site, or sent in an HTML-renderable email message.

Yahoo! Messenger "addview" function allows for the automatic execution of malicious script contained in web pages.

A vulnerability exists in the Yahoo! Messenger "addview" function that permits a remote attacker to execute arbitrary script and HTML in the Internet security zone of the local machine. The "addview" function is only supposed to accept view information from Yahoo! servers. However, an attacker can send malicious script and HTML to the client using the Yahoo! URL redirection service. This script or HTML is interpreted by the Yahoo! Messenger client and is displayed in the client's web browser.

These vulnerabilities were resolved in Yahoo! Messenger version 5,0,0,1065, released May 22, 2002; however, a bug in the distribution server may have inadvertently installed Yahoo! Messenger version 5,0,0,1036 on systems that downloaded Yahoo! Messenger after May 22, 2002. The bug in the distribution server has since been resolved.

All of these vulnerabilities were resolved in Yahoo! Messenger version 5,0,0,1058, released February 25, 2002, or by server-side resolutions around the same time.

Impact:

A remote attacker can execute arbitrary code with the privileges of the victim user, cause a denial of service, or modify data in the victim's "buddy" list.

Solution:

Upgrade to the latest version of Yahoo! Messenger

On May 22, 2002, Yahoo! released a fixed version of Yahoo! Messenger (5,0,0,1065) and began issuing a patch (5,0,0,1066) via the AutoUpdater to address this issue. All users should upgrade to version 5,0,0,1065 or later. Users with versions prior to 5,0,0,1066 that have "Auto Update" enabled will receive a message informing them that an upgrade is available. All users should accept this upgrade.

Users who downloaded Yahoo! Messenger after May 22, 2002, should be aware that a bug in the distribution server might have inadvertently installed Yahoo! Messenger version 5,0,0,1036, which is vulnerable to all issues in this advisory. The bug in the distribution server has since been resolved.

Users should upgrade and verify the version of Yahoo! Messenger by selecting the "About Yahoo! Messenger..." option from the Help menu.

Securiteam: [NT] Multiple Vulnerabilities in Yahoo! Messenger

Implement a firewall and filtering

Yahoo! Messenger listens for peer-to-peer requests on port 5101/TCP but users can implement a firewall to block inbound and outbound access to port 5101/TCP. However, since Yahoo! Messenger URI's can be embedded in a web site or email message, blocking requests to and from port 5101/TCP is not a completely effective solution. Mail and Internet filters should also be applied to filter the "ymsgr:" URI handler from email messages and web sites.

Appendix A. – Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Yahoo!, Inc.

Yahoo! encourages users to upgrade to the latest version whenever prompted by the AutoUpdater or regularly check for updated versions of the client at <http://messenger.yahoo.com> <http://messenger.yahoo.com>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:cert-advisory@cert.org> CERT Advisory.

=====

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

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] SHOUTcast Remote Buffer Overflow (icy-name)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)