

CERT Advisory CA-2002-16 Multiple Vulnerabilities in Yahoo! Messenger

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2002-06/0002.html>

From: CERT Advisory (cert-advisory@cert.org)

Date: 06/05/02

Date: Wed, 5 Jun 2002 15:02:11 -0400 (EDT)
From: CERT Advisory <cert-advisory@cert.org>
To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2002-16 Multiple Vulnerabilities in Yahoo! Messenger

Original release date: June 05, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

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

Overview

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.

I. Description

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:

VU#137115 – Yahoo! Messenger contains a buffer overflow in the URI handler

Cert: CERT Advisory CA-2002-16 Multiple Vulnerabilities in Yahoo! Messenger

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.

This vulnerability has been assigned as CAN-2002-0031 by the Common Vulnerabilities and Exposures (CVE) group:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0031>

VU#172315 – 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.

This vulnerability has been assigned as CAN-2002-0032 by the Common Vulnerabilities and Exposures (CVE) group:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0032>

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.

In February 2002, the following vulnerabilities were reported to affect Yahoo! Messenger:

- * <http://www.kb.cert.org/vuls/id/393195>
- * <http://www.kb.cert.org/vuls/id/419419>
- * <http://www.kb.cert.org/vuls/id/755755>
- * <http://www.kb.cert.org/vuls/id/887319>
- * <http://www.kb.cert.org/vuls/id/952875>

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.

II. Impact

Cert: CERT Advisory CA-2002-16 Multiple Vulnerabilities in Yahoo! Messenger

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.

III. 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 may 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.

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>.

Cert: CERT Advisory CA-2002-16 Multiple Vulnerabilities in Yahoo! Messenger

The CERT Coordination Center thanks Scott Woodward <scott@phoenixtechie.com>, Phuong Nguyen <dphuong@yahoo.com>, and Adam Lang <themeetup@hotmail.com> for their discovery and analysis of these vulnerabilities. We also thank Yahoo! for their assistance in analyzing and responding to these issues.

Feedback can be directed to the author: Jason A. Rafail

Appendix B. – References

1. <http://www.kb.cert.org/vuls/id/137115>
 2. <http://www.kb.cert.org/vuls/id/172315>
 3. <http://www.kb.cert.org/vuls/id/393195>
 4. <http://www.kb.cert.org/vuls/id/419419>
 5. <http://www.kb.cert.org/vuls/id/755755>
 6. <http://www.kb.cert.org/vuls/id/887319>
 7. <http://www.kb.cert.org/vuls/id/952875>
-

This document is available from:

<http://www.cert.org/advisories/CA-2002-16.html>

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email.

Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

Cert: CERT Advisory CA-2002-16 Multiple Vulnerabilities in Yahoo! Messenger

CERT publications and other security information are available from our web site

<http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University.

Revision History

June 05, 2002: Initial release

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8

iQCVAwUBPP5cYaCVPMXQI2HJAQGAUAQAh/Xuz419nzyhbV8Oif1WDa2qczCF8ETW
hYzkQYsi7tXg+kR4GcHfWgFDwlB4F4ojVoe7uBdKfasmQ7lfWXx2V+xxSm7LIbou
6YItFjt8CXPnC6WS+4ODjfr8U+hFRw2AIoUTcewwFT1PMHEMjtunQaiEJkXLqGkM
YAhQ31TZF6Y=

=jGbu

-----END PGP SIGNATURE-----

-
- **Previous message:** [CERT Advisory: "CERT Advisory CA-2002-15 Denial-of-Service Vulnerability in ISC BIND 9"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)