

[VulnWatch] Secunia Research: Yahoo! Messenger File Transfer Filename Spoofing

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-02/0021.html>

From: Andreas Sandblad (*as_at_secunia.com*)

Date: 02/18/05

To: vuln@secunia.com

Date: Fri, 18 Feb 2005 14:59:52 +0100

Secunia Research 18/02/2005

– Yahoo! Messenger File Transfer Filename Spoofing –

Table of Contents

Affected Software.....	1
Severity.....	2
Description of Vulnerability.....	3
Solution.....	4
Time Table.....	5
Credits.....	6
References.....	7
About Secunia.....	8
Verification.....	9

1) Affected Software

Yahoo! Messenger 6.0.0.1750

Other versions may also be affected.

2) Severity

Rating: Less critical

Impact: Spoofing

Where: From remote

3) Description of Vulnerability

VulnWatch: [VulnWatch] Secunia Research: Yahoo! Messenger File Transfer Filename Spoofing

Secunia Research has discovered a vulnerability in Yahoo! Messenger, which can be exploited by malicious people to trick users into executing malicious files.

The problem is that files with long filenames are not displayed correctly in the file transfer dialogs. This can be exploited to trick users into accepting and potentially executing malicious files.

Details:

Yahoo! Messenger wraps overly long filenames and shows only the first line of the filename in the file transfer dialogs. The file extension can thus be spoofed for a filename containing a whitespace and two file extensions.

Successful exploitation requires that the option "Hide extension for known file types" is enabled in Windows (default setting).

The vulnerability has been confirmed in version 6.0.0.1750. Other versions may also be affected.

4) Solution

Update to version 6.0.0.1921.
<http://messenger.yahoo.com/>

5) Time Table

04/01/2005 – Vulnerability discovered.
10/01/2005 – Vendor notified.
19/01/2005 – Vendor confirms the vulnerability.
17/02/2005 – Vendor issued fixed version.
18/02/2005 – Public disclosure.

6) Credits

Discovered by Andreas Sandblad, Secunia Research.

7) References

The Common Vulnerabilities and Exposures (CVE) project has assigned candidate number CAN-2005-0243 for the vulnerability.

8) About Secunia

VulnWatch: [VulnWatch] Secunia Research: Yahoo! Messenger File Transfer Filename Spoofing

Secunia collects, validates, assesses, and writes advisories regarding all the latest software vulnerabilities disclosed to the public. These advisories are gathered in a publicly available database at the Secunia web site:

<http://secunia.com/>

Secunia offers services to our customers enabling them to receive all relevant vulnerability information to their specific system configuration.

Secunia offers a FREE mailing list called Secunia Security Advisories:

http://secunia.com/secunia_security_advisories/

9) Verification

Please verify this advisory by visiting the Secunia web site:

http://secunia.com/secunia_research/2005-2/advisory/
