

[SNS Advisory No.64] IP Messenger for Win Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-05/0131.html>

From: Secure Net Service(SNS) Security Advisory (*snsadv_at_lac.co.jp*)

Date: 05/13/03

Date: Tue, 13 May 2003 13:10:53 +0900

To: bugtraq@securityfocus.com

SNS Advisory No.64

IP Messenger for Win Buffer Overflow Vulnerability

Problem first discovered on: Mon, 24 Mar 2003

Published on: Tue, 13 May 2003

Overview:

IP Messenger for Win ver 2.02 and previous versions are prone to a buffer overflow vulnerability in the file & folder transfer mechanism.

Problem Description:

A buffer overflow occurs when a user attempts to save a file containing an unusually long filename received through IP Messenger for Win.

Remote attackers could take advantage of this flaw to execute code of their choice with the privileges of the IP Messenger user.

Note that versions of IP Messenger that do not support the file & folder transfer mechanism are not affected by this issue.

Tested Versions:

IP Messenger for Win ver 2.00

IP Messenger for Win ver 2.01

IP Messenger for Win ver 2.02

Solution:

It is possible to rectify this problem by upgrading to IP Messenger for Win ver 2.03.

SecurityFocus Bugtraq: [SNS Advisory No.64] IP Messenger for Win Buffer Overflow Vulnerability

<http://www.asahi-net.or.jp/~VZ4H-SRUZ/ipmsg-eng.html>

Discovered by:

Hisayuki Shinmachi

Acknowledgements:

Thanks to:

Hiroaki Shirouzu

Disclaimer:

The information contained in this advisory may be revised without prior notice and is provided as it is. Users shall take their own risk when taking any actions following reading this advisory. LAC Co., Ltd. shall take no responsibility for any problems, loss or damage caused by, or by the use of information provided here.

This advisory can be found at the following URL:

http://www.lac.co.jp/security/english/snsadv_e/64_e.html

SecureNet Service(SNS) Security Advisory <snsadv@lac.co.jp>
Computer Security Laboratory, LAC <http://www.lac.co.jp/security/>