

[Full-disclosure] Microsoft Windows Messenger Remote Illegal Access Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-08/msg00301.html>

- *From:* cocoruder <cocoruder@xxxxxxxxxx>
 - *Date:* Wed, 13 Aug 2008 21:08:31 -0700
-

Microsoft Windows Messenger Remote Illegal Access Vulnerability

by cocoruder(frankruder_at_hotmail.com)
<http://ruder.cdut.net>

Summary:

A remote illegal access vulnerability exists in Microsoft Windows Live Messenger. A vicious attacker can control the Live Messenger via constructing a malicious web page, once the victim visits this page, the attacker can control the local Live Messenger, including disclosing personal sensitive information of Live Messenger, transferring local audio and video information to remote and so on.

Affected Software Versions:

Microsoft Windows Live Messenger 4.7 on Windows XP and Windows Server 2003
Microsoft Windows Live Messenger 5.1 on Windows 2000, Windows XP and Windows Server 2003

Details:

When installing Windows XP, an old edition of MSN Messenger is installed automatically. The old edition opens the MSN API to develop as an ActiveX Control, and marks it with "safe".

By using this ActiveX Control, we can control the local MSN Messenger, for instance: change state, gain current login ID, steal contact-person's information, send mail using the victim's name, and so on, all of these functions given by this feature can be considered to be security problems.

Even the user installs a higher edition of MSN Messenger(Windows Live Messenger), this ActiveX control will not be removed. By using

[Full-disclosure] Microsoft Windows Messenger Remote Illegal Access Vulnerability

this we will still be allowed to visit the local Live Messenger.

Solution:

Microsoft has released an advisory for this vulnerability which can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms08-050.mspx>

CVE Information:

CVE-2008-0082

Disclosure Timeline:

2007.05.31 Vendor notified
2007.05.31 Vendor responded
2008.XX.XX Advisory delayed by the vendor many times
2008.08.12 Coordinated public disclosure

--EOF--

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>