

TopResponse Threat Advisory

Release Date: August 15, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks targeting the Microsoft Windows Messenger UIAutomation ActiveX Vulnerability (MS08-050,CVE-2008-0082).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows Messenger v4.7 and v5.1; Microsoft Windows XP Professional x64 Edition, Microsoft Windows XP SP2, Microsoft Windows 2000 SP4, Microsoft Windows Server 2003 SP1, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2003 x64 Edition, Microsoft Windows Server 2003 x64 Edition SP2, Microsoft Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Windows XP SP3.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: Microsoft Windows Messenger, now known as Windows Live Messenger, is an instant messaging client. The client supports the Microsoft UIAutomation control, which implements a managed code API exposing user interface that can be used for test automation. There exists a vulnerability in the UIAutomation control. The reported vulnerability could allow an attacker to change state, obtain contact information, capture a user's logon ID and initiate video and audio chat sessions without the knowledge of the logged-on user by enticing the user to open a specially crafted web page.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2008-08-13-02 (or later) to put this new protection into place. This is automatically applied to the "Strict Client Protection" IPS Rule Set. In order to take advantage of the protection, make sure the IPS rule tln-106195 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Windows Messenger client infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms08-050.msp

Relevant TLN Rules: tln-106195

Relevant TopResponse Protection Pack(s): 2008-08-13-02