

## TopResponse Threat Advisory

**Release Date:** April 15, 2011.

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Windows Messenger Remote Code Execution Vulnerability (MS11-027,CVE-2011-1243).

**Top Layer Products:** IPS 5500 E-Series.

**Vulnerable Infrastructure:** Microsoft Windows XP SP3, Microsoft Windows XP SP3, Microsoft Windows XP Professional x64 Edition SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2003 x64 Edition SP2, Microsoft Windows Server 2003 with SP2 for Itanium-based Systems,Microsoft Windows Vista SP1 and Microsoft Windows Vista SP2,Microsoft Windows Vista x64 Edition SP1 and Microsoft Windows Vista x64 Edition SP2,Microsoft Windows Server 2008 for 32-bit Systems and Microsoft Windows Server 2008 for 32-bit Systems SP2,Microsoft Windows Server 2008 for x64-based Systems and Microsoft Windows Server 2008 for x64-based Systems SP2,Microsoft Windows Server 2008 for Itanium-based Systems and Microsoft Windows Server 2008 for Itanium-based Systems SP2,Microsoft Windows 7 for 32-bit Systems,Microsoft Windows 7 for 32-bit Systems SP1,Microsoft Windows 7 for x64-based Systems,Microsoft Windows 7 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for x64-based Systems,Microsoft Windows Server 2008 R2 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for Itanium-based Systems,Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1.

**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:** The Microsoft Windows Messenger software (Microsoft Windows Live Messenger and Microsoft Windows MSN Messenger are not affected) is vulnerable to attacks on an ActiveX component implemented by the software. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by enticing the user to open a specially crafted web site.

**Recommended Action:** Top Layer recommends the following actions:

Download and apply Protection Pack 2011-04-13-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Windows Messenger Remote Code Execution Vulnerability that will be applied to the “Recommended Client Protection” IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106356 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Windows Messenger infrastructure.

**References:** Use the following sources for additional information:

Additional Information	Location
Top Layer Support	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/bulletin/ms11-027.msp">http://www.microsoft.com/technet/security/bulletin/ms11-027.msp</a>

**Relevant TLN Rules:** tln-106356.

**Relevant TopResponse Protection Pack(s):** 2011-04-13-01.