



Securing Tomorrow's  
Networks Today

## TopResponse Threat Advisory

**Release Date:** February 17, 2010

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide new protection for known attacks of the Microsoft Windows Shell Handler URL Validation Vulnerability (MS10-007, CVE-2010-0027).

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

**Vulnerable Infrastructure:** Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, Windows Server 2003 with SP2 for Itanium-based Systems.

**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 user interface provides applications, such as networked browsers, an API to the Windows Shell. The vulnerability targets how the ShellExecute function processes specially crafted input parameters. The vulnerability could allow an attacker to execute arbitrary code on the user's system in the context 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 2010-02-16-02 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106302 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your client infrastructure.

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

<b>Additional Information</b>	<b>Location</b>
<b>Top Layer Support</b>	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
<b>Microsoft Support</b>	<a href="http://www.microsoft.com/technet/security/bulletin/ms10-007.msp">http://www.microsoft.com/technet/security/bulletin/ms10-007.msp</a>
<b>Mitre CVE</b>	<a href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0027">http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0027</a>

**Relevant TLN Rules:** tln-106302

**Relevant TopResponse Protection Pack(s):** 2010-02-16-02