

## TopResponse Threat Advisory

**Release Date:** December 9, 2008

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft Internet Explorer HTML Rendering Memory Corruption Vulnerability (CVE-2008-4261; MS08-073).

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

**Vulnerable Infrastructure:** Internet Explorer v5.01, v6, v6 SP1, and v6 SP2; Microsoft Windows 2000 SP4, XP SP3, XP x64 Edition SP2, Server 2003 SP2, Server x64 Edition SP2 and Server 2003 for Itanium SP2.

**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 Internet Explorer is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The ability to embed rich content in web pages is used by many sites. The reported vulnerability targets how Microsoft Internet Explorer handles memory while processing unexpected objects embedded into a web page. The vulnerability could allow a remote attacker to execute arbitrary code on the client system in the context of the logged-on user by enticing the user to open a specially crafted web page. The IPS 5500 provides proactive protection for this vulnerability.

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

Ensure that the rule tln-016002, "EXPLT: Microsoft Windows Media Player Plug-in buffer Overflow Vulnerability", is enabled in the IPS Rule Set that is used to inspect traffic sent to your client infrastructure. The rule is currently enabled in the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets.

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

<b>Additional Information</b>	<b>Location</b>
<b>Top Layer Support Web site</b>	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
<b>Microsoft Advisory</b>	<a href="http://www.microsoft.com/technet/security/bulletin/MS08-073.msp">http://www.microsoft.com/technet/security/bulletin/MS08-073.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4261">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4261</a>

**Relevant TLN Rules:** tln-016002