

## TopResponse Threat Advisory

**Release Date:** December 16, 2008

**Revised Date:** December 17, 2008

**Correction:** IPS 5500 v4.X protection was reported in error. Protection is provided with features only present on the IPS 5500 E-Series.

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks of the Microsoft Internet Explorer XML Parsing Vulnerability (CVE-2008-4844).

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

**Vulnerable Infrastructure:** Microsoft Internet Explorer 7 on Microsoft Windows XP Service Pack 2, Windows XP Service Pack 3, Windows Server 2003 Service Pack 1, Windows Server 2003 Service Pack 2, Windows Vista, and Windows Vista Service Pack 1, and Windows Server 2008.

**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 7 is a common web browser used by Microsoft client infrastructure. The vulnerability is found in mshtml.dll when an XML document containing nested SPAN elements are processed. Delivery of a specially crafted file can be made by an XML formatted email message, an XML formatted web page, or an XML document file attachment. The vulnerability could allow an 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 XML document.

Specific attacks using the Microsoft Internet Explorer XML Parsing vulnerability have emerged and are actively exploiting systems. The IPS 5500 provides proactive protection for several known attacks of this vulnerability.

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

Ensure that the rule tln-025069, “EXPLT: JavaScript Suspicious Code”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft client infrastructure utilizing Microsoft Internet Explorer 7 to browse network content. The rule is currently enabled in the “Strict Client Protection” IPS Rule Set.

In the absence of rule tln-025069, an additional layer of protection is provided by a second rule that will trigger. Ensure that the rule tln-016010, “PROTO: HTML Illegal character found in document body”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft Internet Explorer 7 to browse network content. The rule is currently enabled in the “Strict Client Protection” and “Strict Server Protection” IPS Rule Sets.

Note: IPS 5500 E-Series customer will see rule tln-025069 events rather than rule tln-016010 events when both rules are enabled.

**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/advisory/961051.msp">http://www.microsoft.com/technet/security/advisory/961051.msp</a>
<b>Milw0rm Advisories</b>	<a href="http://www.milw0rm.com/exploits/7403">URL:http://www.milw0rm.com/exploits/7403</a> <a href="http://www.milw0rm.com/exploits/7410">URL:http://www.milw0rm.com/exploits/7410</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4844">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4844</a>

**Relevant TLN Rules:** tln-025069 or tln-016010