

## TopResponse Threat Advisory

**Release Date:** December 16, 2008

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide protection for 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.

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

Download and apply Protection Pack 2008-12-16-01 (or later) to put this new protection into place. Protection for this vulnerability is automatically applied to the “Recommended Client Protection” IPS Rule Set. In order to take advantage of the protection, make sure the IPS rule tln-106220, “EXPLT: Microsoft Internet Explorer XML Parsing Vulnerability” is enabled in the IPS Rule Set used to inspect traffic to your Microsoft client infrastructure.

With Protection Pack 2008-12-16-01 (or later), rule tln-106140, “EXPLT: Javascript Exploit NOP Sled”, has been enhanced and will trigger on known attacks. IPS 5500 E-Series customer will see tln-106140 events rather than the two previously rules listed in the proactive protection advisory for CVE-2008-4844.

Note: Protection Pack 2008-12-16-01 (or later) provides additional protection against post-exploitation attempts by known exploits of the reported vulnerability. The SANS\_DShield blocked IP address list has been updated to incorporate known malicious sites. Ensure that your IPS Unit’s Security Policy table contains a policy row configured to block traffic to or from the SANS\_DShield Host Group.

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

Additional Information	Location
Top Layer Support Web site	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/advisory/961051.mspx">http://www.microsoft.com/technet/security/advisory/961051.mspx</a>
Mitre CVE	<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-106140, tln-106220