

## TopResponse Threat Advisory

**Release Date:** February 15, 2008

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against attacks on the Microsoft Internet Information Services (IIS) ASP Input Vulnerability (MS08-006, CVE-2008-0075).

**Top Layer Products:** IPS 5500 v4.X and higher.

**Vulnerable Infrastructure:** Microsoft IIS v5.1, v6.0; Microsoft Windows XP, Windows Server 2003.

**Alert Type:** Recommendations regarding a recent vulnerability

**Risk Assessment:** Moderate

**Threat Impact:** Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

**Advisory Impact:** Prevention

**Summary:** The Microsoft Internet Information Services (IIS) includes a WWW Publishing Service that implements Active Server Pages (ASP) functionality. One of the methods offered as part of the ASP functionality is the HTMLEncode method of the Server object that is often used by ASP developers to sanitize user input. The reported vulnerability could allow a remote attacker to execute arbitrary code on a vulnerable system by passing a specially crafted input to an ASP page that uses the vulnerable HTMLEncode method. The IPS 5500 provides proactive protection for the vulnerability.

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

1. Ensure that the rule tln-102031, "PROTO: HTTP URI Path Contains Invalid Character", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft IIS infrastructure.

**Note:** This rule is enabled by default in the "Strict Server Protection" IPS Rule Set.

**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 Security Bulletin</b>	<a href="http://www.microsoft.com/technet/security/bulletin/ms08-006.msp">http://www.microsoft.com/technet/security/bulletin/ms08-006.msp</a>

**Relevant TLN Rules:** tln-102031.