

## TopResponse Threat Advisory

**Release Date:** July 11, 2007

**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) Remote Code Execution Vulnerability (MS07-041, CVE-2005-4360).

**Top Layer Products:** IPS 5500 v3.4X and higher.  
IPS 5500 E-Series all versions.

**Vulnerable Infrastructure:** Windows XP Professional SP2.

**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) 5.1 URL parser is vulnerable to attacks using specially crafted URL requests. The vulnerability was originally disclosed as a Denial-of-Service vulnerability. However, additional details have been reported recently that could allow a remote attacker to execute arbitrary code on a vulnerable system. The IPS 5500 provides proactive protection against the published attacks for the vulnerability.

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

1. Install the updated version of the Microsoft Internet Information Services as recommended by the vendor.
2. Ensure that the rule tln-102019, "PROTO: HTTP URI Path Contains Invalid Character", is enabled in the IPS Rule Sets that provide protection for your Microsoft Internet Information Services infrastructure.

**Note:** This rule is enabled by default in the "Strict Server" 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/MS07-041.msp">http://www.microsoft.com/technet/security/Bulletin/MS07-041.msp</a>

**Relevant TLN Rules:** tln-102019.