

## TopResponse Threat Advisory

**Release Date:** June 12, 2008

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against attacks originating from infrastructure compromised using the Microsoft Internet Explorer HTTP Request Header Vulnerability (MS08-031, CVE-2008-1544).

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

**Vulnerable Infrastructure:** Microsoft Internet Explorer v5.01 and Microsoft Internet Explorer v6 SP1; Windows 2000 SP4.

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

**Risk Assessment:** Moderate

**Threat Impact:** Attacks associated with a remotely exploitable vulnerability

**Advisory Impact:** Post-exploitation protection against attacks from vulnerable infrastructure

**Summary:** The Microsoft Internet Explorer provides support for the setRequestHeader() method as part of the XMLHttpRequest object that can be used to modify HTTP request headers. The current restrictions imposed on the method are insufficient. As a result, a remote attacker may be able to stage attacks from vulnerable infrastructure by enticing users to visit a specially crafted web site. The reported vulnerability could allow a remote attacker to perform attacks against servers, including HTTP request splitting attacks and HTTP request smuggling attacks. The IPS 5500 provides proactive protection against the attacks.

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

1. Ensure that the rule tln-102050, "PROTO: HTTP Message Contains Multiple Instances Of A Specified Header", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Web server and Web proxy infrastructure.
2. Ensure that the rule tln-102053, "PROTO: HTTP Header Contains Invalid Character In Unknown Header Name", is enabled in the IPS Rule Set that is used to sent traffic to your Web server and Web proxy infrastructure.

**Note:** These rules are enabled by default in the "Recommended 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/ms08-031.msp">http://www.microsoft.com/technet/security/bulletin/ms08-031.msp</a>

**Relevant TLN Rules:** tln-102050,tln-102053.