

## TopResponse Threat Advisory

**Release Date:** December 10, 2009

**Purpose:** The Top Layer TopResponse team informs customers that after analysis of Microsoft vulnerability details, IPS 5500 security features provide improved protection against the Microsoft Internet Explorer Style Object Remote Code Execution Vulnerability (MS09-072, CVE-2009-3672, BID37085).

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

**Vulnerable Infrastructure:** Microsoft Internet Explorer v7, Microsoft Internet Explorer v6.01 and Microsoft Internet Explorer v6.0.

**Alert Type:** Critical Vulnerabilities

**Risk Assessment:** Critical

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

**Advisory Impact:** Prevention

**Summary:** Microsoft Internet Explorer is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The reported vulnerability targets how Microsoft Internet Explorer handles the processing of style objects. The vulnerability could allow a remote 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 web page.

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

Download and apply Protection Pack 2009-12-09-02 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106288 is enabled in the IPS Rule Set used to inspect HTML traffic sent to your Microsoft systems that have the vulnerable versions of Microsoft Internet Explorer enabled.

**Note:** The advisory published on November 23, 2009 designated rules currently enabled in the Strict IPS Rule Sets for protection of publically release vulnerability details. The improved protection is enabled in the Recommended IPS Rule Set and is less likely to have false positive events.

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

<b>Additional Information</b>	<b>Location</b>
<b>Top Layer Support</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/Bulletin/MS09-072.msp">http://www.microsoft.com/technet/security/Bulletin/MS09-072.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3672">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3672</a>
<b>SecurityFocus BID</b>	<a href="http://www.securityfocus.com/bid/37085">http://www.securityfocus.com/bid/37085</a>

**Relevant TLN Rules:** tln-106288