



Securing Tomorrow's  
Networks Today

## TopResponse Threat Advisory

**Release Date:** March 31, 2010

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide new protection for the Microsoft Internet Explorer Memory Corruption Vulnerability (MS10-018, CVE-2010-0805).

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

### **Vulnerable Infrastructure:**

Internet Explorer 5.01 on Microsoft Windows 2000 SP4; Internet Explorer 6 on Microsoft Windows 2000 SP4, Windows XP SP3, and Windows XP Professional x64 Edition SP2.

**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 is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The vulnerability targets how Microsoft Internet Explorer handles a long URL processed by a loaded ActiveX control. 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 2010-03-31-01 (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-106310 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure.

**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 Support</b>	<a href="http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp">http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0805">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0805</a>

**Relevant TLN Rules:** tln-106310

**Relevant TopResponse Protection Pack(s):** 2010-03-31-01