

## TopResponse Threat Advisory

**Release Date:** August 12, 2010.

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Internet Explorer Uninitialized Memory Corruption (MS10-053,CVE-2010-2556) and Microsoft Internet Explorer Event Handler Cross-Domain (MS10-053,CVE-2010-1258) Vulnerabilities.

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

**Vulnerable Infrastructure:** Microsoft Internet Explorer 6 for Windows XP SP3, Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition SP2, Microsoft Internet Explorer 6 for Windows Server 2003 SP2, Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition SP2, Microsoft Internet Explorer 6 for Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Internet Explorer 7, and other software as specified in the Microsoft bulletin describing the vulnerability.

**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 contains code that is vulnerable to attacks that involve accessing deleted or improperly created objects and running scripts that access other browser windows. The reported Microsoft Internet Explorer vulnerabilities could allow an attacker to disclose information and to execute arbitrary code on the users systems 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:

### **IPS 5500 E-Series Users:**

Download and apply Protection Pack 2010-08-12-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Internet Explorer Uninitialized Memory Corruption and Microsoft Internet Explorer Event Handler Cross-Domain Vulnerabilities that will be applied to the "Recommended Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rules tln-106327 and tln-106328 are enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure.

**Note:** Both IPS rules tln-106327 and tln-106328 are currently enabled in the Strict IPS Rule Sets because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

To manually enable one of these rules in a IPS Rule Set complete the following steps:

1. Log into the Web Management Interface of your IPS 5500 E-Series.
  2. Select **Configure Security->Security Policies**.
  3. Select the **IPS Rule Sets** tab.
  4. Select the Rule Set for which you want to change the setting of rule tln-106327.
  5. Enter **tln-106327** in the search window.
  6. Double click on the rule **tln-106327 EXPLT: Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability**.
  7. Make sure that the **Enabled** button is checked.
  8. Make sure that the **Action** is set to **DROP**.
  9. Click the **OK** button.
- Repeat steps 4 through 9 for all other Rule Sets that you want to change.
10. Close the Configure Security Policies window.  
Click the **Save** icon (upper left of your GUI).

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

Additional Information	Location
<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/MS10-053.mspx">http://www.microsoft.com/technet/security/bulletin/MS10-053.mspx</a>

**Relevant TLN Rules:** tln-106327, tln-106328

**Relevant TopResponse Protection Pack(s):** 2010-08-12-01