

## TopResponse Threat Advisory

**Release Date:** December 22, 2008

**Purpose:** The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the Microsoft Internet Explorer Parameter Validation Vulnerability (MS08-073,CVE-2008-4258).

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

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

**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 reported vulnerability targets how Microsoft Internet Explorer handles memory while processing certain navigation methods embedded into a web page. 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 2008-12-22-01 (or later) to put this new protection into place. Protection for this vulnerability is automatically applied to the "Strict Client Protection" and "Strict Server Protection" IPS Rule Sets.

In order to take advantage of the protection, make sure the IPS rule tln-106222 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft client infrastructure.

To manually enable this rule in any 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 106222
  5. Enter **106222** in the search window
  6. Double click on the rule **tlN-106222 EXPLT: Microsoft IE Parameter Validation 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
  11. Click the **Save** icon (upper left of your GUI).

**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 Advisory</b>	<a href="http://www.microsoft.com/technet/security/bulletin/MS08-073.msp">http://www.microsoft.com/technet/security/bulletin/MS08-073.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4258">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4258</a>

**Relevant TLN Rules:** tlN-106222