



Securing Tomorrow's  
Networks Today

## TopResponse Threat Advisory

**Release Date:** June 9, 2010

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide new protection for the Microsoft Internet Explorer toStaticHTML Information Disclosure Vulnerability (MS10-035, MS10-039, CVE-2010-1257).

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

### **Vulnerable Infrastructure:**

Internet Explorer 8 for Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, and Windows Server 2003 x64 Edition SP2, Windows Vista SP2, Windows Vista x64 Edition SP2, Windows Server 2008 for 32-bit, Itanium-based, and x64-based Systems SP2, Windows 7 for 32-bit and x64-based Systems, and Windows Server 2008 R2 for x64-based and Itanium-based Systems;

Microsoft Office InfoPath 2003 SP3, Microsoft Office InfoPath 2007 SP1 and SP2, Microsoft Office SharePoint Server 2007 SP1 and SP2 for 32-bit and 64-bit editions, as well as Microsoft Windows SharePoint Services 3.0 SP1 and SP2 for 32-bit and 64-bit editions.

**Alert Type:** Information Disclosure

**Risk Assessment:** High

**Threat Impact:** Remotely exploitable vulnerability that could allow an attacker to read arbitrary files on the 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 domain restrictions for remote requests to read cached data. The vulnerability could allow an attacker to read arbitrary files on the user's 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 2010-06-09-02 (or later) to put this new protection into place. This is automatically applied to the “Strict Client Protection” IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106317 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure.

**Note:** The IPS rule tln-106317 is 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 this rule 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-106317.
5. Enter **tln-106317** in the search window.
6. Double click on the rule **tln-106317 EXPLT: Microsoft Internet Explorer toStaticHTML Information Disclosure 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</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/MS10-035.msp">http://www.microsoft.com/technet/security/Bulletin/MS10-035.msp</a> <a href="http://www.microsoft.com/technet/security/Bulletin/MS10-039.msp">http://www.microsoft.com/technet/security/Bulletin/MS10-039.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1257">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1257</a>

**Relevant TLN Rules:** tln-106317

**Relevant TopResponse Protection Pack(s):** 2010-06-09-02