

## TopResponse Threat Advisory

**Release Date:** August 17, 2007

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks for the Microsoft XML Core Services substringData ActiveX (CVE-2007-2223) Vulnerability.

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

**Vulnerable Infrastructure:** Microsoft Internet Explorer v5.01, v6 SP1, and v7.

**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 XML Core Services (MSXML) allows customers who use JScript, Visual Basic Scripting Edition (VBScript), and Microsoft Visual Studio 6.0 to develop XML-based applications that provide interoperability with other applications that adhere to the XML 1.0 standard. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the security 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 2007-08-16-02 (or later) to put this new protection into place. This is automatically applied to the "Strict Client Protection" Rule Set. If you are using other Rule Sets to inspect HTTP traffic (many users will typically use the recommended rule sets) then apply the manual instructions below to these other Rule Sets to enable this rule.

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 106156
  5. Enter **106156** in the search window
  6. Double click on the rule **tlN-106156 EXPLT: Microsoft XML Core Svc substringData ActiveX Overflow**
  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/ms07-042.msp">http://www.microsoft.com/technet/security/bulletin/ms07-042.msp</a>

**Relevant TLN Rules:** TLN-106156

**Relevant TopResponse Protection Pack(s):** 2007-08-16-02