

## TopResponse Threat Advisory

**Release Date:** November 16, 2006

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks for the Microsoft XML Core Services XMLHTTP SetRequestHeader() Vulnerability (CVE-2006-5745).

**Top Layer Products:** IPS 5500 Version 3.40 and higher.

**Vulnerable Infrastructure:** Microsoft XML Core Services 4.0, Microsoft XML Core Services 6.0; Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Server 2003.

**Alert Type:** Targeted protection

**Risk Assessment:** Critical

**Threat Impact:** Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems.

**Advisory Impact:** Prevention

**Summary:** The Microsoft XML Core Services (MSXML) framework provides implementations of XML, XML Schema, XPath, and XSLT. One of the most popular applications that uses the framework is Microsoft Internet Explorer. There exists a vulnerability in the Microsoft XML Core Services XMLHTTP ActiveX control that could allow an attacker to execute arbitrary code on the user's system in the security context of the logged-on user by enticing the user to visit a specially crafted web page.

**Recommended Action:** Top Layer recommends the following actions to protect the vulnerable infrastructure:

**TopResponse™ Users:** Download and apply Protection Pack 2006-11-13-03 (or later). No further action is needed.

**IPS 5500 Manual Configuration Instructions if you are not using TopResponse™**

**Note:** There are different instructions for IPS 5500 Version 3.40 and Version 4.X.

### Instructions for Version 3.40:

Version 3.40 users should complete the following steps:

1. Log into the Web Management Interface of your IPS 5500.
2. Select **IPS Configuration->Filter Configuration->Payload Signatures->Patterns**.
3. Click the **Add** button.
4. Enter the following for the new entry:

**Note:** *If you have not created the HTTP-Client string set yet, as described in the TopResponse WMF Advisory from December 29, 2005, you should do so before proceeding.*

Signature:

|25 75 39 30 39 30|

String Set:

**HTTP-Client**

ID Label:

**111306.NOP.1**

5. Click the **Done** button.
6. Click the **Close** button.
7. Click the **Apply** button.
8. Click the **Save** button.

### Instructions for Version 4.X:

Version 4.X users should complete the following steps:

1. Log into the Web Management Interface of your IPS 5500.
2. Select **Configure Security->Advanced Security Config->IPS Rules Customization->->Attack Signatures->Patterns**.
3. Click the **Add** button.
4. Enter the following for the new entry:

**Note:** *If you have not created the HTTP-Client string set yet, as described in the TopResponse WMF Advisory from December 29, 2005, you should do so before proceeding.*

Signature:

|25 75 39 30 39 30|

String Set:

**HTTP-Client**

ID Label:

**111306.NOP.1**

5. Click the **Done** button.
6. Click the **Apply** button.
7. Click the **Close** button.
8. Click the **Save** icon (upper left of your GUI).

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

Additional Information	Location
Top Layer Support Web site	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/bulletin/ms06-071.msp">http://www.microsoft.com/technet/security/bulletin/ms06-071.msp</a>

**Relevant TLN Rules:** TLN-106140

**Relevant TopResponse Protection Pack(s):** 2006-11-13-03