

## TopResponse Threat Advisory

**Release Date:** November 12, 2008

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft XML Core Services Cross-Domain Disclosure (MS08-069,CVE-2008-4029).

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

**Vulnerable Infrastructure:** Microsoft XML Core Services 3.0, Microsoft XML Core Services 4.0;

**Alert Type:** Critical vulnerability

**Risk Assessment:** Moderate

**Threat Impact:** Information Disclosure

**Advisory Impact:** Prevention

**Summary:** Microsoft Windows includes Microsoft XML Core Services (formerly known as MSXML) that provides support for XML and XSL content processing. The Microsoft XML Core Services component includes the ability to load external Document Type Definitions (DTD). There exists a vulnerability in the way the Microsoft XML Core Services component handles error checking for external DTDs. The reported vulnerability could allow an attacker to gain access to sensitive information from the users systems by enticing a user to access a specially crafted web page.

**Recommended Action:** Top Layer recommends the following actions:

Download and apply Protection Pack 2008-11-11-02 (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, make sure the IPS rule tln-106209 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft XML Core Services client infrastructure.

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

Additional Information	Location
<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/MS08-069.msp">http://www.microsoft.com/technet/security/bulletin/MS08-069.msp</a>

**Relevant TLN Rules:** tln-106209

**Relevant TopResponse Protection Pack(s):** 2008-11-11-02