

## TopResponse Threat Advisory

**Release Date:** April 15, 2009

**Purpose:** The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the Microsoft DirectShow MJPEG Code Execution Vulnerability (MS09-011, CVE-2009-0084).

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

**Vulnerable Infrastructure:** DirectX v8.1 running on Microsoft Windows 2000 SP4; DirectX v9.0 running on Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows XP Professional x64 Edition and Windows XP Professional x64 Edition SP2, Microsoft Windows Server 2003 SP1 and Windows Server 2003 SP2, Microsoft Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition SP2, Microsoft Windows Server 2003 with SP1 for Itanium-based Systems, and Microsoft Windows Server 2003 with SP2 for Itanium-based Systems.

**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:** DirectX is a component of the Microsoft Windows operating System that enable graphics, sound and video in applications. DirectShow is an Application Programming Interface (API) to these media controls. The reported vulnerability targets how Microsoft DirectShow handles the decompression of an MJPEG media file. 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 file.

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

Download and apply Protection Pack 2009-04-14-04 (or later) to put this new protection into place. Protection for this vulnerability 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-106236 “EXPLT: Microsoft DirectShow MJPEG Code Execution Vulnerability” is enabled in the IPS Rule Set used to inspect traffic that transfers MJPEG media files 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 106236
5. Enter **106236** in the search window
6. Double click on the rule **tln-106236 EXPLT: Microsoft DirectShow MJPEG Code Execution 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/MS09-011.msp">http://www.microsoft.com/technet/security/bulletin/MS09-011.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0084">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0084</a>

**Relevant TLN Rules:** tln-106236

**Relevant TLN Protection Pack:** 2009-04-14-04