

## TopResponse Threat Advisory

**Release Date:** June 1, 2009

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for the Microsoft DirectShow Remote Code Execution Vulnerability (CVE-2009-1537).

**Top Layer Products:** IPS 5500 E-Series running V5.20.028 (or later).

**Vulnerable Infrastructure:** Microsoft Windows 2004 SP4, Microsoft Windows XP, and Microsoft Windows Server 2003.

**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 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 the Quicktime media file format. The vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by enticing the user to open a specially crafted Quicktime media file which was attached to an email, linked on a web site, or downloaded directly from the network.

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

Download and apply Protection Pack 2009-06-01-02 (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-106245 is enabled in the IPS Rule Set used to inspect traffic that transfers Quicktime media files to your client infrastructure.

**Note:** The IPS rule tln-106245 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-106245.
  5. Enter **106245** in the search window.
  6. Double click on the rule **tln-106245 EXPLT: Microsoft DirectShow Remote 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/advisory/971778.msp">http://www.microsoft.com/technet/security/advisory/971778.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1537">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1537</a>

**Relevant TLN Rules:** tln-106245

**Relevant TopResponse Protection Pack(s):** 2009-06-01-02

**Relevant Top Layer Software Version(s):** V5.20.028 or later