

## TopResponse Threat Advisory

**Release Date:** May 15, 2009

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for the Microsoft PowerPoint ExEmbed Memory Corruption Vulnerability (MS09-017, CVE-2009-0225).

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

**Vulnerable Infrastructure:** Microsoft Office PowerPoint 2002 SP3.

**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 PowerPoint is a presentation application that is used to display graphics, formatted text, videos and other media on pre-arranged slides. The slides are stored in the PowerPoint Presentation (PPT) file format. There is a vulnerability in the processing of the Microsoft PPT file format; specifically, the vulnerability involves the process of the older PowerPoint 95 file format. The reported 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 PPT file which was attached to an email or downloaded directly from the network.

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

Download and apply Protection Pack 2009-05-13-01 (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-106239 is enabled in the IPS Rule Set used to inspect traffic that may contain PowerPoint (PPT) documents.

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 106239
  5. Enter **106239** in the search window
  6. Double click on the rule **tlN-106239 EXPLT: Microsoft Powerpoint PP7 Memory Corruption 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/ms09-017.msp">http://www.microsoft.com/technet/security/bulletin/ms09-017.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0225">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0225</a>

**Relevant TLN Rules:** tlN-106239

**Relevant TopResponse Protection Pack(s):** 2009-05-13-01