

## TopResponse Threat Advisory

**Release Date:** May 11, 2011.

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft Powerpoint Presentation Remote Code Execution Vulnerability (MS11-036,CVE-2011-1269).

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

**Vulnerable Infrastructure:** Microsoft PowerPoint 2002 SP3, Microsoft PowerPoint 2003 SP3, Microsoft PowerPoint 2007 SP2, Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, Open XML File Format Converter for Mac, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2.

**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 contains a vulnerability that involves parsing of Powerpoint (PPT) files with malformed fields. 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 a user to open a specially crafted PPT file. The IPS 5500 provides proactive protection for this vulnerability.

In order to take advantage of the protection, customers should make sure the IPS rule tln-106280 is enabled in the IPS Rule Set used to inspect client traffic that may contain PowerPoint documents.

**Note:** IPS rule tln-106280 is currently enabled in the Strict IPS Rule Set because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

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

<b>Additional Information</b>	<b>Location</b>
<b>Top Layer Support</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/MS11-036.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-036.msp</a>

**Relevant TLN Rules:** tln-106280.