

## TopResponse Threat Advisory

**Release Date:** June 15, 2009

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Excel Record Integer Overflow Vulnerability (MS09-021,CVE-2009-0561).

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

**Vulnerable Infrastructure:** Microsoft Office Excel 2000 SP3, Microsoft Office Excel 2002 SP3, Microsoft Office Excel 2003 SP3, Microsoft Office Excel 2007 SP1 and SP2, Microsoft Office Excel Viewer, as well as, the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2..

**Alert Type:** Critical vulnerability

**Risk Assessment:** Moderate

**Threat Impact:** Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

**Advisory Impact:** Prevention

**Summary:** Microsoft Excel supports the ability to store information in a spreadsheet file format. There is an exploitable defect in the way that Microsoft Office Excel parses the Excel file format records. The reported vulnerability could allow an 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 XLS file.

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

Download and apply Protection Pack 2009-06-11-01 (or later) to put this new protection into place. This is automatically applied to the "Strict Client Protection" and "Strict Server Protection" IPS Rule Sets.

In order to take advantage of the protection, make sure the IPS rule tln-106248 "EXPLT: Microsoft Excel Record Integer Overflow Vulnerability" is enabled in the IPS Rule Set used to inspect traffic that transfers Microsoft Excel document files to your client infrastructure.

**Note:** The IPS rule tln-106248 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-106248.
  5. Enter **106248** in the search window.
  6. Double click on the rule **tln-106246 EXPLT: Microsoft Excel Record Integer Overflow 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:

Additional Information	Location
<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/MS09-021.msp">http://www.microsoft.com/technet/security/Bulletin/MS09-021.msp</a>
<b>Mitre CVE</b>	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0561">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0561</a>

**Relevant TLN Rules:** tln-106248

**Relevant TopResponse Protection Pack(s):** 2009-06-11-01