

## TopResponse Threat Advisory

**Release Date:** June 15, 2010

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Office Excel Record Stack Corruption Vulnerability (MS10-038, CVE-2010-1251).

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

**Vulnerable Infrastructure:** Microsoft Office XP SP3, Microsoft Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2.

**Alert Type:** Important Vulnerability

**Risk Assessment:** Important

**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 corrupted Excel records contained within stored XLS files. 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 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 2010-06-15-05 (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, customers should make sure the IPS rule tln-106319 is enabled in the IPS Rule Set used to inspect traffic that may contain Excel (XLS) documents.

**Note:** The IPS rule tln-106319 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-106319.
  5. Enter **tln-106319** in the search window.
  6. Double click on the rule **tln-106319 EXPLT: Microsoft Excel Record Stack 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</b>	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
<b>Microsoft Support</b>	<a href="http://www.microsoft.com/technet/security/bulletin/ms10-038.msp">http://www.microsoft.com/technet/security/bulletin/ms10-038.msp</a>
<b>Mitre CVE</b>	<a href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1251">http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1251</a>

**Relevant TLN Rules:** tln-106319

**Relevant TopResponse Protection Pack(s):** 2010-06-15-05