

TopResponse Threat Advisory

Release Date: March 9, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Office Excel MDXSET Record Heap Overflow Vulnerability (MS10-017, CVE-2010-0261).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office Excel 2007 SP1 and Microsoft Office Excel 2007 SP2; Microsoft Office Excel Viewer SP1 and Microsoft Office Excel Viewer SP2; Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats 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 the Excel MDXSET 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 2010-03-09-02 (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, customers should make sure the IPS rule tln-106307 is enabled in the IPS Rule Set used to inspect traffic that may contain Excel (XLS) documents.

Note: The IPS rule tln-106307 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-106307.
 5. Enter **tln-106307** in the search window.
 6. Double click on the rule **tln-106307 EXPLT: Microsoft Office Excel MDXSET Record Heap 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
Top Layer Support	http://www.toplayer.com/support
Microsoft Support	http://www.microsoft.com/technet/security/bulletin/ms10-017.msp
Mitre CVE	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0261

Relevant TLN Rules: tln-106307

Relevant TopResponse Protection Pack(s): 2010-03-09-02