



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: May 11, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide new protection for the Microsoft VBE6 Stack Memory Corruption Vulnerability (MS10-031, CVE-2010-0815).

Top Layer Products: IPS 5500 E-Series

Vulnerable Infrastructure: Microsoft Office XP SP3, Microsoft Office 2003 SP3, Microsoft Office System SP1, Microsoft Office System SP2, Microsoft Visual Basic for Applications, and Microsoft Visual Basic for Applications SDK.

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 data fields defining external OLE objects. 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 2010-05-11-01 (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, customers should make sure the IPS rule tln-106313, "EXPLT: Microsoft VBE6 Stack Memory Corruption Vulnerability", is enabled in the IPS Rule Set used to inspect traffic that transfers Powerpoint (PPT) files to your client infrastructure.

Note: The IPS rule tln-106313 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-106313.
 5. Enter **tln-106313** in the search window.
 6. Double click on the rule **tln-106313 EXPLT: Microsoft VBE6 Stack 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:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Support	http://www.microsoft.com/technet/security/Bulletin/MS10-031.msp
Mitre CVE	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0815

Relevant TLN Rules: tln-106313

Relevant TopResponse Protection Pack(s): 2010-05-11-01