



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: August 16, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Silverlight Memory Corruption Vulnerability (MS10-060,CVE-2010-0019).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Silverlight 3 when installed on Mac, Microsoft Silverlight 3 when installed on all releases of Microsoft Windows clients, and Microsoft Silverlight 3 when installed on all releases of Microsoft Windows servers.

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 Silverlight is a cross-browser, cross-platform web application framework that enables building rich interactive applications and provides functionality similar to the one offered in Adobe Flash. The functionality offered enables applications to integrate graphics, animations, and interactivity in a single runtime environment. The reported Microsoft Silverlight 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 web page.

Recommended Action: Top Layer recommends the following actions:

IPS 5500 E-Series Users:

Download and apply Protection Pack 2010-08-13-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Silverlight Memory Corruption Vulnerability that will be applied to the "Strict Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106329 is enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure.

Note: IPS rules tln-106329 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.

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-106329.
5. Enter **tln-106329** in the search window.
6. Double click on the rule **tln-106329 EXPLT: Microsoft Silverlight 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 Advisory	http://www.microsoft.com/technet/security/bulletin/MS10-060.msp

Relevant TLN Rules: tln-106329

Relevant TopResponse Protection Pack(s): 2010-08-13-01