

TopResponse Threat Advisory

Release Date: November 23, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against the Microsoft Internet Explorer Style Object Remote Code Execution Vulnerability (BID37085).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Internet Explorer v7, Microsoft Internet Explorer v6.01 and Microsoft Internet Explorer v6.0.

Alert Type: Critical Vulnerabilities

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: Microsoft Internet Explorer is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The reported vulnerability targets how Microsoft Internet Explorer handles the processing of style objects. The vulnerability could allow a remote 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 web page. The IPS 5500 provides proactive protection for known attacks of this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rules tln-025069, “EXPLT: Javascript Suspicious Code”, and tln-016010, “PROTO: HTML Illegal character found in document body”, are enabled in the IPS Rule Set that is used to inspect HTML traffic sent to your Microsoft systems that have the vulnerable versions of Microsoft Internet Explorer enabled. These rules are currently enabled in the “Strict Client Protection” IPS Rule Set.

Note: The IPS rules tln-016010 and tln-025069 are 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-016010**.
5. Enter **tln-016010** in the search window.
6. Double click on the rule **tln-016010 PROTO: HTML Illegal character found in document body**.
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. Select the Rule Set for which you want to change the setting of rule **tln-025069**.
11. Enter **tln-025069** in the search window.
12. Double click on the rule **tln-025069 EXPLT: Javascript Suspicious Code**.
13. Make sure that the **Enabled** button is checked.
14. Make sure that the **Action** is set to **DROP**.
15. Click the **OK** button.

Repeat steps 10 through 15 for all other Rule Sets that you want to change.

16. Close the Configure Security Policies window.
17. 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
Security Focus BID	http://www.securityfocus.com/bid/37085

Relevant TLN Rules: tln-016010 and tln-025069