

TopResponse Threat Advisory

Release Date: January 6, 2011.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block know attacks targeting the Microsoft Internet Explorer CSS Clip Remote Code Execution Vulnerability (MS10-090,CVE-2010-3962).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Internet Explorer v6, v7, and v8 as specified in the Microsoft advisory for the vulnerability.

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 Internet Explorer implements the Microsoft HTML engine that performs parsing of HTML content. There is a vulnerability in the way HTML pages containing specially crafted CSS tags are parsed by the engine. 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 visit a specially crafted web site.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2011-01-05-02 (or later) to put this new protection into place. This will put into place protection for the Microsoft Internet Explorer CSS Clip Remote Code Execution Vulnerability that will be applied to the “Recommended Client Protection” IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-025117 is enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure.

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/ms10-090.msp

Relevant TLN Rules: tln-025117

Relevant TopResponse Protection Pack(s): 2011-01-05-02