



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: December 16, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Internet Explorer HTML Memory Corruption (MS10-090,CVE-2010-3345) and Microsoft Internet Explorer HTML Onload Memory Corruption (MS10-090,CVE-2010-3346) Vulnerabilities.

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Internet Explorer 6 for Windows XP SP3, Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition SP2, Microsoft Internet Explorer 6 for Windows Server 2003 SP2, Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition SP2, Microsoft Internet Explorer 8 for Windows XP SP3, Microsoft Internet Explorer 8 for Windows XP Professional x64 Edition SP2, Microsoft Internet Explorer 8 for Windows Server 2003 SP2, and other software versions as specified in the Microsoft bulletin describing the vulnerability.

Alert Type: Critical Vulnerabilities

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 capabilities that enable dynamic object insertion and accessing objects before the page is completely loaded. There are flaws in the implementation of these capabilities that could enable remote code execution. The reported vulnerabilities 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 2010-12-16-04 (or later) to put this new protection into place. This will put into place protection for the Microsoft Internet Explorer HTML Memory Corruption and Microsoft Internet Explorer HTML Onload Memory Corruption vulnerabilities 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 rules tln-106344 and tln-106345 are enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure.

Note: IPS rules tln-106344 and tln-106345 are currently enabled in the Strict IPS Rule Set because there is a potential for false positive events. Please monitor events after the rules are enabled to provide protection for this vulnerability.

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-106344,tln-106345

Relevant TopResponse Protection Pack(s): 2010-12-16-04