



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: March 11, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide new protection for the Microsoft Internet Explorer Object Type Attribute Remote Code Execution Vulnerability (CVE-2010-0806).

Top Layer Products: IPS 5500 E-Series

Vulnerable Infrastructure:

Internet Explorer 6 on Microsoft Windows 2000 SP4, Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 SP2 for Itanium-based and x64 Edition SP2;

Internet Explorer 7 for Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 SP2 for Itanium-based Systems, Windows Server 2003 x64 Edition SP2, Windows Vista SP2, Windows Vista x64 Edition SP2, Windows Server 2008 for 32-bit, Itanium-based, and x64-based Systems SP2;

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 is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The vulnerability targets how Microsoft Internet Explorer handles the management of Object Type attributes. Protected Mode in Internet Explorer of Windows Vista (and later) limits the effectiveness of the attack. 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.

Detailed information and a proof of concept attack using the Microsoft Internet Explorer Object Type Attribute Remote Code Execution vulnerability have emerged and are publicly available.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2010-03-10-03 (or later) to put this new protection into place. This is automatically applied to the “Recommended Client Protection” IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106308 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure.

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/advisory/981374.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806

Relevant TLN Rules: tln-106308

Relevant TopResponse Protection Pack(s): 2010-03-10-03