

TopResponse Threat Advisory

Release Date: September 8, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft DHTML Editing Component ActiveX Vulnerability (MS09-046,CVE-2009-2519).

Top Layer Products: IPS 5500 E-Series

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, and Windows Server 2003 with SP2 for Itanium-based Systems.

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: The Microsoft DHTML Editing Component ActiveX Control provides users an HTML editor for updating dynamic web sites. Microsoft reports that this control is not intended to be used in Internet Explorer, but can be loaded at the request of a remote web site. The 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:

Download and apply Protection Pack 2009-09-08-03 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets. In order to take advantage of the protection, customers should make sure the IPS rule tln-106269 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 Advisory	http://www.microsoft.com/technet/security/Bulletin/MS09-046.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2519

Relevant TLN Rules: tln-106269

Relevant TopResponse Protection Pack(s): 2009-09-08-03