

## TopResponse Threat Advisory

**Release Date:** July 6, 2010.

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to block known attacks targeting the Microsoft Windows Help HCP Code Execution Vulnerability (CVE-2010-1885).

**Top Layer Products:** IPS 5500 E-Series.

**Vulnerable Infrastructure:** Microsoft Windows XP Service Pack 2 and Windows XP Service Pack 3, Microsoft Windows XP Professional x64 Edition Service Pack 2, Microsoft Windows Server 2003 Service Pack 2, Microsoft Windows Server 2003 x64 Edition Service Pack 2, and Microsoft 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:** Microsoft Help and Support Center is the application used by Microsoft to access online documentation by default. There is a vulnerability in the implementation of the application's whitelist mechanism used to filter help documents and parameters passed on the command line. 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 open a specially crafted web site.

**Recommended Action:** Top Layer recommends the following actions:

**IPS 5500 E-Series Users:** Download and apply Protection Pack 2010-07-02-04 (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, make sure the IPS rule tln-106321 is enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure

**References:** Use the following sources for additional information:

<b>Additional Information</b>	<b>Location</b>
<b>Top Layer Support</b>	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
<b>Microsoft Advisory</b>	<a href="http://www.microsoft.com/technet/security/advisory/2219475.mspx">http://www.microsoft.com/technet/security/advisory/2219475.mspx</a>

**Relevant TLN Rules:** tln-106321

**Relevant TopResponse Protection Pack(s):** 2010-07-02-04