



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: March 2, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide new protection for known attacks of the Microsoft Windows VBScript HLP Remote Code Execution Vulnerability (CVE-2010-0483).

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, 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 Windows HLP file format provides applications, such as Internet Explorer, many methods to display help information to the end user. The vulnerability targets how the VBScript functions are called within Windows HLP files opened using Internet Explorer. The vulnerability could allow an attacker to execute arbitrary code on the user's system 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 2010-03-02-02 (or later) to put this new protection into place. This is automatically applied to the "Strict Client Protection" and "Strict Server Protection" IPS Rule Sets. In order to take advantage of the protection, customers should make sure the IPS rule tln-106304, "EXPLT: Microsoft VBScript HLP Remote Code Execution Vulnerability", is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your client infrastructure.

Note: The IPS rule tln-106304 is currently enabled in the Strict IPS Rule Sets because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

To manually enable this rule in a IPS Rule Set complete the following steps:

1. Log into the Web Management Interface of your IPS 5500 E-Series.
 2. Select **Configure Security->Security Policies**.
 3. Select the **IPS Rule Sets** tab.
 4. Select the Rule Set for which you want to change the setting of rule tln-106304.
 5. Enter **tln-106304** in the search window.
 6. Double click on the rule **tln-106304 EXPLT: Microsoft VBScript HLP Remote Code Execution Vulnerability**.
 7. Make sure that the **Enabled** button is checked.
 8. Make sure that the **Action** is set to **DROP**.
 9. Click the **OK** button.
- Repeat steps 4 through 9 for all other Rule Sets that you want to change.
10. Close the Configure Security Policies window.
 11. Click the **Save** icon (upper left of your GUI).

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/981169.mspx
Mitre CVE	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0483

Relevant TLN Rules: tln-106304

Relevant TopResponse Protection Pack(s): 2010-03-02-02