

TopResponse Threat Advisory

Release Date: July 27, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Windows Shell LNK Remote Code Execution Vulnerability (CVE-2010-2568).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows XP Professional x64 Edition Service SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2003 x64 Edition SP2, Microsoft Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Windows Vista Service Pack 1 and Windows Vista SP2, and other software as described in the Microsoft bulletin.

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 user interface (UI) provides users with access to objects needed for running applications and managing the operating system. Microsoft Windows Shell organizes these objects into a hierarchical namespace and provides users and applications with a consistent and efficient way to access and manage objects. The reported Microsoft Windows Shell LNK 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 shortcut file.

Recommended Action: Top Layer recommends the following actions:

IPS 5500 E-Series Users:

Download and apply Protection Pack 2010-07-27-04 (or later) to put this new protection into place. This will put into place protection for known attacks targeting the Microsoft Windows Shell LNK Remote Code Execution Vulnerability. In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106324 is enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure.

Note: The IPS rule tln-106324 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-106324.
5. Enter **tln-106324** in the search window.
6. Double click on the rule **tln-106324 EXPLT: Microsoft Windows Shell LNK 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.

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 Advisory	http://www.microsoft.com/technet/security/advisory/2286198.mspx

Relevant TLN Rules: tln-106324.

Relevant TopResponse Protection Pack(s): 2010-07-27-04.