

TopResponse Threat Advisory

Release Date: October 25, 2007

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks for the Microsoft Sharepoint Cross-site Scripting Vulnerability (CVE-2007-2581).

Top Layer Products: IPS 5500 v4.X and higher.
IPS 5500 E-Series all versions

Vulnerable Infrastructure: Microsoft Windows Sharepoint Services v3.0 for Windows Server 2003, Microsoft Office Sharepoint Server 2007.

Alert Type: Remotely Exploitable Vulnerability

Risk Assessment: Moderate

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: The Microsoft Windows SharePoint Services is a technology provided in Windows Server 2003 that supports a platform for collaboration applications, offering a common framework for document management and a common repository for storing documents of all types. The reported vulnerability could allow an attacker to execute arbitrary script code on vulnerable systems by sending a specially crafted HTTP request.

Recommended Action: Top Layer recommends the following actions:

IPS 5500 and IPS 5500 E-Series Users: Download and apply Protection Pack 2007-10-22-02 (or later) to put this new protection into place. The rule tln-102066 that provides protection is enabled by default in the "Strict Server Protection" IPS Rule Set. If you are using other Rule Set(s) to inspect HTTP traffic then apply the manual instructions below to these other Rule Set(s) to enable this rule.

To manually enable this rule in any 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 102066
 5. Enter **102066** in the search window
 6. Double click on the rule **tlN-102066 AAUPV: HTTP URI File Name Matches Specified Filter**
 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 Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms07-059.msp

Relevant TLN Rules: TLN-102066

Relevant TopResponse Protection Pack(s): 2007-10-22-02